Manual de producto de GFI

GFI EventsManager™

Guía del administrador

GFI®

La información y contenido de este documento se proporciona sólo para fines informativos y se proporciona "tal cual", sin garantía de ningún tipo, ya sea expresa o implícita, incluyendo pero no limitadas a las garantías implícitas de comercialización, idoneidad para un propósito particular y ausencia de infracción. GFI Software no se hace responsable de ningún daño, incluyendo daños consecuentes, de cualquier naturaleza, que puedan deberse a la utilización de este documento. La información se ha obtenido de fuentes disponibles públicamente. A pesar de los esfuerzos razonables que se han hecho para asegurar la exactitud de los datos facilitados, GFI no reclama, promete o garantiza la integridad, exactitud, actualidad o adecuación de la información y no es responsable de errores tipográficos, fuera de la información actualizada, o errores. GFI no ofrece ninguna garantía, expresa o implícita, y no asume ninguna obligación legal ni responsabilidad por la exactitud o la exhaustividad de la información contenida en este documento.

Si estima que existe algún error objetivo en este documento, póngase en contacto con nosotros y revisaremos sus dudas tan pronto como sea posible.

Todos los nombres de productos y empresas que se mencionan aquí pueden ser marcas comerciales de sus respectivos propietarios.

GFI EventsManager es propiedad de GFI SOFTWARE Ltd. - 1999-2013 GFI Software Ltd. Reservados todos los derechos.

Versión del documento: 13.0.0

Última actualización (mes/día/año): 3/18/2014

Tabla de contenido

1 Introducción **21**

1.1 Acerca de GFI EventsManager 21
1.2 Cómo funciona GFI EventsManager 23
1.2.1 Etapa 1: Recopilación de eventos 24
1.2.2 Etapa 2: Procesamiento de eventos 24
1.3 Convenciones utilizadas en esta guía 25

2 Instalación de GFI EventsManager **26**

2.1 Escenario de implementación 26
2.1.1 GFI EventsManager en una Red de área local (LAN) 28
2.1.2 GFI EventsManager en una zona desmilitarizada (DMZ) 29
2.1.3 GFI EventsManager en una red de área extensa (WAN) 31
2.2 Requisitos del sistema 32
2.2.1 Requisitos de hardware 32
2.2.2 Sistemas operativos admitidos (32 y 64 bits) 32
2.2.3 Otros componentes de software 33
2.2.4 Requisitos de almacenamiento 33
2.2.5 Puertos y protocolos del firewall 33
2.2.6 Permisos del firewall 34
2.2.7 Configuración de orígenes de eventos 34
2.2.8 Excepciones del antivirus 35
2.2.9 Consideraciones de identificación de equipos 35
2.2.10 Recopilar registros de eventos desde equipos que ejecutan Microsoft® Vista o una versión posterior 35
2.3 Actualizar GFI EventsManager 36
2.3.1 Actualizar desde una versión anterior 36
2.4 Instalar una nueva instancia de GFI EventsManager 45
2.4.1 Procedimiento de instalación 45
2.5 Probar la instalación 54
2.5.1 Eventos del proceso - Equipo local 55
2.5.2 Eventos del proceso - Dominio local 57
2.5.3 Eventos de proceso - Máquinas seleccionadas 60

3 Obtención de resultados **63**

3.1 Lograr la seguridad de la red 63
3.2 Supervisar eficientemente el estado del sistema 65
3.3 Lograr el cumplimiento con PCI DSS 67

4 Administrar orígenes de eventos **69**

4.1 Agregar orígenes de eventos manualmente 69
4.2 Agregar orígenes de eventos automáticamente 70
4.3 Crear un nuevo grupo de orígenes de eventos 73
4.4 Configurar propiedades de orígenes de eventos 75
4.4.1 Configurar propiedades generales de orígenes de eventos 75
4.4.2 Configurar credenciales de inicio de sesión de orígenes de eventos 76

4.4.3 Configurar el tipo de licencia de los orígenes de eventos 78
4.4.4 Configurar el tiempo operativo de los orígenes de eventos 80
4.4.5 Configurar la supervisión de orígenes de eventos 81
4.4.6 Configurar parámetros de procesamiento de eventos 83
4.5 Orígenes de bases de datos 84
4.5.1 Orígenes de Microsoft®SQL Server® 84
4.5.2 Orígenes de Oracle Server 92

5 Recopilar registros de eventos 103

5.1 Recopilar registros de eventos de Windows® 103
5.2 Recopilar registros de texto 106
5.3 Recopilar Syslogs 109
5.3.1 Configurar puerto de comunicaciones del servidor Syslog 112
5.4 Recopilar mensajes de capturas SNMP 113
5.4.1 Configurar servidor de capturas SNMP 116
5.5 Recopilar registros personalizados 117
5.6 Recopilar registros de eventos de GFI LanGuard 119
5.6.1 Cómo habilitar el registro de eventos de GFI LanGuard 120
5.7 Recopilar eventos de GFI EndPointSecurity 124

6 Buscar eventos almacenados 126

6.1 Desplazarse en el Explorador de eventos 126
6.2 Usar el Explorador de eventos 127
6.2.1 Exportar eventos a CSV 127
6.2.2 Crear informes a partir de vistas 128
6.2.3 Eliminar eventos 129
6.2.4 Buscar eventos almacenados 130
6.2.5 Identificar reglas mediante la herramienta de búsqueda de reglas 130
6.3 Administrar vistas en el Explorador de eventos 130
6.3.1 Crear vistas raíz y vistas 131
6.3.2 Editar una vista 133
6.3.3 Eliminar una vista 134
6.4 Personalizar el diseño del Explorador de eventos 134
6.4.1 Personalizar la posición de descripción 134
6.4.2 Opciones de codificación de colores de eventos 134
6.5 Buscar eventos desde diferentes bases de datos 136

7 Supervisión de actividades 137

7.1 Vista de estado general 137
7.2 Vista de actividad de tareas 141
7.3 Vista de estadísticas 143

8 Generación de informes 145

8.1 Desplazarse por la ficha Reports 146
8.2 Informes disponibles 147
8.3 Administrar informes 149
8.3.1 Crear una carpeta raíz 149

8.3.2 Crear una carpeta 151
8.4 Crear un informe raíz 151
8.5 Crear informes personalizados 157
8.6 Generar informes 164
8.6.1 Generar un informe 164
8.6.2 Generar informes de resumen diarios 165
8.6.3 Generar informes de configuración 167
8.6.4 Generar informes de reglas 169
8.6.5 Generar informes del historial operativo 170
8.6.6 Generar informes de descripción general de actividades 172
8.7 Analizar informes 174
8.8 Definir encabezados de columna 175
8.8.1 Generar informes de eventos de distintas bases de datos 176
8.9 Personalizar informes HTML 176

9 Reglas de procesamiento de eventos 179

9.1 Acerca de las reglas de procesamiento de eventos 179
9.1.1 Clasificación de eventos 180
9.2 Administrar carpetas de conjuntos de reglas 181
9.2.1 Conjuntos de reglas disponibles 181
9.2.2 Agregar una carpeta de conjuntos de reglas 183
9.2.3 Renombrar y eliminar una carpeta de conjunto de reglas 183
9.3 Crear nuevas reglas de procesamiento de eventos 184
9.4 Crear nuevas reglas desde eventos existentes 189
9.5 Parámetros de filtro avanzado de eventos 194
9.5.1 Parámetros de filtrado de eventos de Windows® 194
9.5.2 Parámetros de filtrado de syslog 194
9.6 Priorizar reglas de procesamiento de eventos 195

10 Supervisión activa 196

10.1 Acerca de las comprobaciones de supervisión activa 196
10.2 Crear y configurar una carpeta raíz 198
10.3 Agregar subcarpetas a una carpeta raíz 202
10.4 Crear y configurar comprobaciones de supervisión activa 207
10.5 Aplicar comprobaciones de supervisión activa 213
10.6 Eliminar carpetas y comprobaciones de supervisión 215

11 Alertas y acciones predeterminadas 216

11.1 Configurar acciones de clasificación predeterminadas 216
11.2 Configurar opciones de alerta 218
11.2.1 Alertas por correo electrónico 220
11.2.2 Alertas a través de la red 221
11.2.3 Alertas por SMS 222
11.2.4 Alertas a través de SNMP 223
11.2.5 Configuración general 223

12 Grupos de usuarios 225

12.1 Configurar la cuenta del administrador 225

12.2 Administrar cuentas de usuario 232
12.2.1 Crear una nueva cuenta de usuario 232
12.2.2 Cambiar propiedades de la cuenta de usuario 238
12.2.3 Eliminar una cuenta de usuario 239
12.3 Administrar grupos de usuarios 239
12.3.1 Crear un nuevo grupo 239
12.3.2 Cambiar propiedades de un grupo 241
12.3.3 Eliminar un grupo 241

13 Opciones de auditoría y seguridad de la consola 242

13.1 Activar sistema de inicio de sesión 242
13.1.1 Recuperación de contraseña 244
13.2 Ocultación de identidad 245
13.3 Auditar actividad de la consola 248
13.4 Credenciales de detección automática 249

14 Mantenimiento de base de datos 252

14.1 Administrar back-end de base de datos 252
14.1.1 Crear una nueva base de datos 252
14.1.2 Proteger su base de datos 253
14.1.3 Hashing de registro de base de datos 255
14.1.4 Cambiar de base de datos de almacenamiento de archivos 257
14.1.5 Configurar opciones de rotación de bases de datos 260
14.1.6 Configurar operaciones de base de datos 261
14.2 Crear tareas de mantenimiento 262
14.2.1 Importar desde archivo 263
14.2.2 Exportar a un archivo 267
14.2.3 Exportar a SQL 271
14.2.4 Copiar datos 276
14.2.5 Confirmar eliminaciones 279
14.2.6 Importar desde la base de datos de SQL Server® 282
14.2.7 Importar desde archivos heredados 286
14.2.8 Importar desde almacenamiento de archivos heredados 290
14.3 Editar tareas de mantenimiento 292
14.3.1 Ver tareas de mantenimiento programadas 292
14.3.2 Editar propiedades de las tareas de mantenimiento 293
14.3.3 Cambiar prioridad de las tareas de mantenimiento 295
14.3.4 Eliminar una tarea de mantenimiento 295

15 Configurar la Consola de administración 296

15.1 Opciones de rendimiento 296
15.2 Actualizaciones del producto 297
15.2.1 Descargar actualizaciones directamente 298
15.2.2 Descargar actualizaciones desde una ubicación alternativa (sin conexión) 299
15.3 Licencias del producto 305
15.3.1 Actualizar una clave de licencia 305
15.3.2 Obtener una clave de licencia de prueba de 30 días gratuita 306

15.3.3 Ver detalles de la licencia ... 306
15.3.4 Comprar una clave de licencia ... 306
15.4 Información de versión del producto ... 307
15.4.1 Comprobar su versión de GFI EventsManager ... 307
15.4.2 Comprobar si hay versiones nuevas ... 307
15.5 Importar y exportar configuraciones ... 308
15.5.1 Exportar configuraciones a un archivo ... 308
15.5.2 Importar configuraciones desde un archivo ... 310
15.5.3 Importar configuraciones desde otra instancia ... 312
15.6 Diseñar restricciones de consulta ... 314
15.6.1 Usar el cuadro de diálogo Edit Query Restriction ... 315

16 Herramientas de la línea de comandos ... 319

16.1 Usar ESMCmdConfig.exe ... 319
16.1.1 /op:registerService ... 320
16.1.2 /op:enable ... 320
16.1.3 /op:disable ... 320
16.1.4 /op:SetLicense ... 320
16.1.5 /op:configureAlerting ... 321
16.1.6 /op:setAdminEmail ... 321
16.1.7 /op:createProgramGroupShortcuts ... 321
16.1.8 /op:removeProgramGroupShortcuts ... 322
16.1.9 /op:getComputers ... 322
16.2 Usar EsmDlibM.exe ... 322
16.2.1 /importFromSQL ... 323
16.2.2 /importFromDlib ... 323
16.2.3 /copyData ... 324
16.2.4 /importFromLegacyFile ... 326
16.2.5 /exportToFile ... 326
16.2.6 /importFromFile ... 328
16.2.7 /commitDeletedRecords ... 330
16.2.8 /exoportToSQL ... 330
16.3 Usar DLibAdm.exe ... 331
16.3.1 /decryptDatabase ... 332
16.3.2 /encryptDatabase ... 332
16.3.3 /displayAllDLib ... 332
16.3.4 /copyMoveDLib ... 333
16.4 Usar EsmReport.exe ... 333
16.4.1 Generar informes de configuración ... 334
16.4.2 Generar informes de estado ... 335
16.4.3 Generar informes de eventos ... 335
16.4.4 Usar ImportSettings.exe ... 336
16.4.5 Usar ExportSettings.exe ... 337

17 Varios ... 339

17.1 Activar permisos de orígenes de eventos manualmente ... 339
17.1.1 Activar permisos en Microsoft® Windows® XP ... 339

17.1.2 Activar permisos en Microsoft® Windows® Vista 340
17.1.3 Activar permisos en Microsoft® Windows® 7 343
17.1.4 Activar permisos en Microsoft® Windows® Server 2003 345
17.1.5 Activar permisos en Microsoft® Windows® Server 2008 (incluido R2) 346
17.2 Activar permisos de orígenes de eventos automáticamente 347
17.2.1 Activar permisos en Windows® Server 2003 a través de GPO 347
17.2.2 Activar permisos en Windows® Server 2008 a través de GPO 348
17.3 Desactivar Control de cuentas de usuario (UAC) 352

18 Solución de problemas **353**

18.1 Documentación 353
18.2 GFI SkyNet 353
18.3 Solicitar soporte técnico 353
18.4 Foro en la red 353
18.5 Asistente para el solucionador de problemas 354

19 Glosario **360**

20 Índice **364**

Lista de figuras

Captura de pantalla 1: GFI EventsManager se integra en cualquier infraestructura de TI existente 21
Captura de pantalla 2: Las etapas operativas de GFI EventsManager 23
Captura de pantalla 3: Exportar datos desde sitios remotos a la instancia principal de GFI EventsManager .. 31
Captura de pantalla 4: Comprobación de requisitos previos a la actualización 37
Captura de pantalla 5: Servidor de base de datos DLib 38
Captura de pantalla 6: EULA del servidor de base de datos DLib 38
Captura de pantalla 7: Carpeta de instalación de DLib 39
Captura de pantalla 8: Iniciar instalación del servidor de base de datos DLib 39
Captura de pantalla 9: Eliminar archivos de la versión anterior 40
Captura de pantalla 10: Pantalla de bienvenida del asistente de instalación de GFI EventsManager 40
Captura de pantalla 11: EULA de GFI EventsManager 41
Captura de pantalla 12: Detalles del registro de GFI EventsManager 41
Captura de pantalla 13: Credenciales de inicio de sesión remoto para supervisión de registros de eventos .. 42
Captura de pantalla 14: Carpeta de instalación de GFI EventsManager 43
Captura de pantalla 15: Se completó la instalación de GFI EventsManager 43
Captura de pantalla 16: Comprobación automática de actualizaciones 44
Captura de pantalla 17: Definir el back-end de la base de datos 44
Captura de pantalla 18: Comprobación de requisitos previos a la actualización 46
Captura de pantalla 19: Servidor de base de datos DLib 47
Captura de pantalla 20: EULA del servidor de base de datos DLib 47
Captura de pantalla 21: Carpeta de instalación de DLib 48
Captura de pantalla 22: Iniciar instalación del servidor de base de datos DLib 48
Captura de pantalla 23: Pantalla de bienvenida del asistente de instalación de GFI EventsManager 49
Captura de pantalla 24: EULA de GFI EventsManager 50
Captura de pantalla 25: Detalles del registro de GFI EventsManager 50
Captura de pantalla 26: Credenciales de inicio de sesión remoto para supervisión de registros de eventos .. 51
Captura de pantalla 27: Carpeta de instalación de GFI EventsManager 52
Captura de pantalla 28: Se completó la instalación de GFI EventsManager 52
Captura de pantalla 29: Comprobación automática de actualizaciones 53
Captura de pantalla 30: Definir el back-end de la base de datos 53
Captura de pantalla 31: Ejecutar GFI EventsManager por primera vez 54
Captura de pantalla 32: Eventos del proceso - Equipo local 55
Captura de pantalla 33: Acciones principales de la consola 56
Captura de pantalla 34: Eventos del proceso - Dominio local 57
Captura de pantalla 35: Asistente de detección automática 58
Captura de pantalla 36: Seleccionar los tipos de orígenes de eventos que desea detectar en la red 58
Captura de pantalla 37: Buscar el progreso de red 59
Captura de pantalla 38: Eventos de proceso - Máquinas seleccionadas 60

Captura de pantalla 39: Agregar nuevo asistente de origen de eventos 61
Captura de pantalla 40: Agregar nuevo asistente de origen de eventos 69
Captura de pantalla 41: Ficha Synchronization properties - General 71
Captura de pantalla 42: Excluir equipos de la sincronización automática 72
Captura de pantalla 43: Ficha Synchronization properties -Schedule 73
Captura de pantalla 44: Agregar un nuevo grupo de orígenes de eventos 74
Captura de pantalla 45: Cuadro de diálogo de propiedades de orígenes de eventos 76
Captura de pantalla 46: Configurar credenciales de inicio de sesión alternativas 77
Captura de pantalla 47: Configurar el tipo de licencia de los orígenes de eventos 79
Captura de pantalla 48: Especificar tiempo operativo 80
Captura de pantalla 49: Ficha Event source properties - Monitoring 82
Captura de pantalla 50: Fichas de configuración de procesamiento de eventos 83
Captura de pantalla 51: Grupos de servidores de base de datos 84
Captura de pantalla 52: Configurar parámetros de inicio de sesión en la ficha Logon Credentials 85
Captura de pantalla 53: Configurar horas normales de trabajo de la ficha Operational Time 86
Captura de pantalla 54: Configurar auditoría de SQL Server en la ficha SQL Server Audit 87
Captura de pantalla 55: Agregar nuevo servidor de Microsoft® SQL 89
Captura de pantalla 56: Propiedades de la base de datos de Microsoft® SQL: Ficha General 90
Captura de pantalla 57: Propiedades de la base de datos de Microsoft® SQL: Ficha Connection Settings 91
Captura de pantalla 58: Propiedades de la base de datos de Microsoft® SQL: Ficha Settings 92
Captura de pantalla 59: Grupos de servidores de base de datos 93
Captura de pantalla 60: Ficha Oracle Database group - General 94
Captura de pantalla 61: Ficha Oracle Database group - Logon Credentials 95
Captura de pantalla 62: Ficha Oracle Database group - Operational Time 96
Captura de pantalla 63: Ficha Oracle Database group - Oracle Audit 97
Captura de pantalla 64: Agregar nuevo servidor Oracle 98
Captura de pantalla 65: Ficha Oracle Server properties - General 99
Captura de pantalla 66: Ficha Oracle Server properties - Connection Settings 100
Captura de pantalla 67: Ficha Oracle Server properties - Audit by Objects 101
Captura de pantalla 68: Ficha Oracle Server properties - Audit by Statements 102
Captura de pantalla 69: Propiedades del grupo de equipos: Configurar parámetros de registros de eventos de Windows® 104
Captura de pantalla 70: Seleccionar registros de eventos que desea recopilar 105
Captura de pantalla 71: Configurar parámetros de procesamiento del registro de eventos de Windows 106
Captura de pantalla 72: Opciones de registros de texto 107
Captura de pantalla 73: Agregar carpetas que contienen registros de texto 108
Captura de pantalla 74: Se deben dirigir los mensajes Syslog al equipo que ejecuta GFI EventsManager. 110
Captura de pantalla 75: Recopilar Syslogs - Opciones de Syslogs 111
Captura de pantalla 76: Configurar puerto de comunicaciones del servidor Syslog 112
Captura de pantalla 77: Opciones de servidor Syslog 113

Captura de pantalla 78: Se deben dirigir los mensajes de captura SNMP al equipo que ejecuta GFI EventsManager. 114
Captura de pantalla 79: Recopilar capturas SNMP 115
Captura de pantalla 80: Configurar capturas SNMP 116
Captura de pantalla 81: Opciones de capturas SNMP 117
Captura de pantalla 82: Configuración de registros de eventos personalizados 118
Captura de pantalla 83: Cuadro de diálogo Custom event logs 119
Captura de pantalla 84: Habilitar el inicio de sesión de GFI LanGuard a través del registro de Windows 121
Captura de pantalla 85: Agregar registros de aplicación de Windows® 122
Captura de pantalla 86: Agregar reglas de GFI LanGuard 123
Captura de pantalla 87: Explorador de eventos 126
Captura de pantalla 88: Herramienta de exportación de eventos 128
Captura de pantalla 89: Botón Report from view 128
Captura de pantalla 90: Herramienta de búsqueda de eventos 130
Captura de pantalla 91: Generador de vista personaliza 131
Captura de pantalla 92: Editar restricción de vista 132
Captura de pantalla 93: Ficha Customize View 133
Captura de pantalla 94: Muestra: Vistas y vistas raíz nuevas 133
Captura de pantalla 95: Personalizar la descripción del explorador 134
Captura de pantalla 96: Configurar la codificación de colores 134
Captura de pantalla 97: Filtro de color avanzado 135
Captura de pantalla 98: Cuadro de diálogo Switch database 136
Captura de pantalla 99: Estado de GFI EventsManager: Vista general 138
Captura de pantalla 100: Estado de GFI EventsManager: Vista de actividad de tareas 142
Captura de pantalla 101: Estado de GFI EventsManager: Vista de estadísticas 143
Captura de pantalla 102: Desplazarse por la interfaz de informes 146
Captura de pantalla 103: Cuadro de diálogo Create Report Folder 150
Captura de pantalla 104: Crear un informe raíz 152
Captura de pantalla 105: Configurar opciones de diseño del nuevo informe raíz 153
Captura de pantalla 106: Insertar un gráfico en un nuevo informe raíz 154
Captura de pantalla 107: Configurar programación de generación de informes 155
Captura de pantalla 108: Opciones para crear nuevo informe 156
Captura de pantalla 109: Configuración de límite de registro 157
Captura de pantalla 110: Crear un informe raíz 158
Captura de pantalla 111: Configurar opciones de diseño del nuevo informe raíz 159
Captura de pantalla 112: Insertar un gráfico en un nuevo informe raíz 160
Captura de pantalla 113: Configurar programación de generación de informes 161
Captura de pantalla 114: Opciones para crear nuevo informe 162
Captura de pantalla 115: Configuración de límite de registro 163
Captura de pantalla 116: Generar un informe 164

Captura de pantalla 117: Muestra de informe 165
Captura de pantalla 118: Configuración de resumen diario por correo electrónico 166
Captura de pantalla 119: Resumen diario por correo electrónico 167
Captura de pantalla 120: Generar informe de configuración 168
Captura de pantalla 121: Muestra de informe de configuración 169
Captura de pantalla 122: Generar informe de configuración 170
Captura de pantalla 123: Informe del historial operativo 171
Captura de pantalla 124: Cuadro de diálogo del historial operativo 171
Captura de pantalla 125: Muestra de informe del historial operativo 172
Captura de pantalla 126: Descripción general de la actividad: Botón para exportar 172
Captura de pantalla 127: Cuadro de diálogo de descripción general de actividades 173
Captura de pantalla 128: Muestra de informe de descripción general de actividad 173
Captura de pantalla 129: Analizar informes 174
Captura de pantalla 130: Definir condiciones de columnas personalizadas 175
Captura de pantalla 131: Cuadro de diálogo Switch database 176
Captura de pantalla 132: Editar plantillas de informes HTML 177
Captura de pantalla 133: Cómo funcionan las reglas de procesamiento de eventos 180
Captura de pantalla 134: Carpeta de conjuntos de reglas y conjuntos de reglas 181
Captura de pantalla 135: Crear una nueva regla 184
Captura de pantalla 136: Seleccionar los registros a los que se aplicará la regla 185
Captura de pantalla 137: Configurar condiciones de la regla 186
Captura de pantalla 138: Seleccionar ocurrencia e importancia del evento 187
Captura de pantalla 139: Seleccionar acción activada 188
Captura de pantalla 140: Crear una regla a partir de un evento existente 190
Captura de pantalla 141: Nueva regla a partir de un evento - Configuración general 191
Captura de pantalla 142: Nueva regla a partir de un evento - Seleccionar registros que desea recopilar 192
Captura de pantalla 143: Nueva regla a partir de un evento - Agregar condiciones 193
Captura de pantalla 144: Cómo funcionan las comprobaciones de supervisión activa 197
Captura de pantalla 145: Estructura de carpeta raíz y subcarpetas 198
Captura de pantalla 146: Ficha Folder properties - General 199
Captura de pantalla 147: Ficha Folder properties - Target computer 199
Captura de pantalla 148: Ficha Folder properties - Schedule 200
Captura de pantalla 149: Ficha Folder Properties - Action events 201
Captura de pantalla 150: Ficha Folder properties - General 202
Captura de pantalla 151: Ficha Folder properties - Target computer 203
Captura de pantalla 152: Ficha Folder properties - Schedule 204
Captura de pantalla 153: Ficha Folder Properties - Action events 205
Captura de pantalla 154: Crear una nueva comprobación de supervisión activa 207
Captura de pantalla 155: Seleccionar tipo de comprobación 208
Captura de pantalla 156: Configurar propiedades generales de comprobación 208

Captura de pantalla 157: Configurar parámetros de comprobación de supervisión 209
Captura de pantalla 158: Seleccionar orígenes efectuados 210
Captura de pantalla 159: Definir el intervalo de tiempo del análisis 211
Captura de pantalla 160: Configurar acciones de registro de eventos 212
Captura de pantalla 161: Ficha Target computers 213
Captura de pantalla 162: Eliminar carpetas y comprobaciones de supervisión 215
Captura de pantalla 163: Configurar acciones de clasificación predeterminadas 216
Captura de pantalla 164: Cuadro de diálogo Default Classification Actions 217
Captura de pantalla 165: Configurar opciones de alerta 219
Captura de pantalla 166: Configurar opciones de correo electrónico 220
Captura de pantalla 167: Configurar opciones de red 221
Captura de pantalla 168: Configurar alertas a través de la red: Dar formato a mensaje 221
Captura de pantalla 169: Configurar opciones de SMS 222
Captura de pantalla 170: Configurar alertas a través de capturas SNMP 223
Captura de pantalla 171: Configurar cuenta EventsManagerAdministrator 226
Captura de pantalla 172: Propiedades de EventsManagerAdministrator 227
Captura de pantalla 173: Configurar horas de trabajo habituales del usuario 228
Captura de pantalla 174: Configurar alertas fuera del horario de trabajo 229
Captura de pantalla 175: Seleccione el grupo del cual es miembro la cuenta de usuario 230
Captura de pantalla 176: Configurar privilegios de la cuenta de usuario 231
Captura de pantalla 177: Filtrar cuenta de usuario 232
Captura de pantalla 178: Crear un nuevo usuario 233
Captura de pantalla 179: Crear un nuevo usuario - Propiedades generales 233
Captura de pantalla 180: Crear un nuevo usuario - Horas de trabajo 234
Captura de pantalla 181: Crear un nuevo usuario - Opciones de alerta 235
Captura de pantalla 182: Crear un nuevo usuario - Seleccionar grupos de notificación 236
Captura de pantalla 183: Crear un nuevo usuario - Privilegios 237
Captura de pantalla 184: Opciones de filtrado de usuarios 238
Captura de pantalla 185: Crear un nuevo grupo de usuarios 239
Captura de pantalla 186: Crear un nuevo grupo de usuarios - Propiedades generales 240
Captura de pantalla 187: Crear un nuevo grupo de usuarios - Propiedades generales 241
Captura de pantalla 188: Editar opciones de seguridad de la consola 243
Captura de pantalla 189: Habilitar sistema de inicio de sesión de EventsManager 244
Captura de pantalla 190: Solicitud de credenciales de inicio de sesión 245
Captura de pantalla 191: Activar la consola de anonimización 246
Captura de pantalla 192: Opciones de anonimización 247
Captura de pantalla 193: Activar auditoría de actividad del usuario de la consola 248
Captura de pantalla 194: Cuadro de diálogo Audit Options 249
Captura de pantalla 195: Configurar credenciales de detección automática 250
Captura de pantalla 196: Especifique las credenciales de detección automática 251

Captura de pantalla 197: Cuadro de diálogo File storage system 253
Captura de pantalla 198: Editar configuración de almacenamiento de archivos 254
Captura de pantalla 199: Habilitar el cifrado 255
Captura de pantalla 200: Activar o desactivar hashing de registros 256
Captura de pantalla 201: Cuadro de diálogo Record hashing 257
Captura de pantalla 202: Ficha Options 258
Captura de pantalla 203: Cambiar de base de datos desde el panel 259
Captura de pantalla 204: Configurar opciones de rotación de bases de datos 260
Captura de pantalla 205: Cuadro de diálogo Database Operations Options 262
Captura de pantalla 206: Crear tareas de importación/exportación 264
Captura de pantalla 207: Importar desde archivo 264
Captura de pantalla 208: Importar desde archivo: Especificar ruta del archivo de importación 265
Captura de pantalla 209: Descifrar archivos de importación seguros 265
Captura de pantalla 210: Agregar condiciones de filtrado 266
Captura de pantalla 211: Ejecutar opciones de tarea 267
Captura de pantalla 212: Crear tareas de importación/exportación 268
Captura de pantalla 213: Exportar a un archivo 268
Captura de pantalla 214: 269
Captura de pantalla 215: Descifrar/Cifrar datos 269
Captura de pantalla 216: Filtrar datos exportados 270
Captura de pantalla 217: Ejecutar opciones de tarea 271
Captura de pantalla 218: Crear tareas de importación/exportación 272
Captura de pantalla 219: Exportar a SQL 273
Captura de pantalla 220: Especificar detalles de SQL Server 273
Captura de pantalla 221: Seleccionar columnas que desea exportar 274
Captura de pantalla 222: Filtrar datos exportados 275
Captura de pantalla 223: Ejecutar opciones de tarea 276
Captura de pantalla 224: Crear tareas de importación/exportación 277
Captura de pantalla 225: Seleccionar tarea de copia de datos 277
Captura de pantalla 226: Especificar bases de datos de origen y destino 278
Captura de pantalla 227: Descifrar y cifrar las bases de datos de origen y destino 278
Captura de pantalla 228: Filtrar datos exportados 279
Captura de pantalla 229: Crear tareas de importación/exportación 280
Captura de pantalla 230: Crear tareas de confirmación de eliminación 281
Captura de pantalla 231: Seleccionar la base de datos de la que desea eliminar los registros. 281
Captura de pantalla 232: Crear tareas de importación/exportación 282
Captura de pantalla 233: Seleccionar Import from SQL Server Database 283
Captura de pantalla 234: Especificar dirección y datos de acceso a SQL Server 283
Captura de pantalla 235: Descifrar bases de datos anonimizadas 284
Captura de pantalla 236: Agregar condiciones de filtrado para filtrar datos no deseados 285

Captura de pantalla 237: Especificar cuándo se ejecuta la tarea de mantenimiento 286
Captura de pantalla 238: Crear tareas de importación/exportación 287
Captura de pantalla 239: Importar desde archivos heredados 287
Captura de pantalla 240: Especificar ubicación del archivo de importación 288
Captura de pantalla 241: Descifrar información en el archivo de importación 288
Captura de pantalla 242: Quitar anonimización 289
Captura de pantalla 243: Filtrar eventos no deseados por medio de condiciones de filtrado 289
Captura de pantalla 244: Especificar cuándo se ejecuta la tarea de mantenimiento 290
Captura de pantalla 245: Crear tareas de importación/exportación 291
Captura de pantalla 246: Importar datos desde almacenamiento de archivos heredados 291
Captura de pantalla 247: Especificar cuándo se ejecuta la tarea de mantenimiento 292
Captura de pantalla 248: Actividad de las tareas de mantenimiento 293
Captura de pantalla 249: Ver las tareas de mantenimiento programadas 293
Captura de pantalla 250: Cuadro de diálogo Maintenance job properties 294
Captura de pantalla 251: Prioridades de las tareas de mantenimiento 295
Captura de pantalla 252: Opciones de rendimiento deGFI EventsManager 296
Captura de pantalla 253: Cuadro de diálogo Performance Options 297
Captura de pantalla 254: Configurar opciones de actualización automática 298
Captura de pantalla 255: Configurar el servidor proxy para descargar las actualizaciones del producto 299
Captura de pantalla 256: Actualizaciones de GFI EventsManager 301
Captura de pantalla 257: Repositorio de actualizaciones de GFI EventsManager 302
Captura de pantalla 258: Abrir CMD en el modo de administrador 303
Captura de pantalla 259: Cambiar ruta de acceso al directorio de instalación de GFI EventsManager. 304
Captura de pantalla 260: Iniciar manualmente una sesión de actualización 304
Captura de pantalla 261: Estado de las actualizaciones 305
Captura de pantalla 262: Cuadro de diálogo Update license key 306
Captura de pantalla 263: Botón para comprar 306
Captura de pantalla 264: Pantalla Version Information 307
Captura de pantalla 265: Exportar configuraciones a un archivo 309
Captura de pantalla 266: Especificar destino de la exportación 309
Captura de pantalla 267: Seleccionar configuraciones de exportación 310
Captura de pantalla 268: Importar configuraciones desde un archivo 311
Captura de pantalla 269: Especificar ubicación del archivo de configuración 311
Captura de pantalla 270: Seleccionar las configuraciones que desea importar 312
Captura de pantalla 271: Importar configuraciones desde otra instancia de GFI EventsManager 313
Captura de pantalla 272: Especificar la ubicación de instancia 313
Captura de pantalla 273: Seleccione las configuraciones que desea importar desde otra instancia de GFI EventsManager. 314
Captura de pantalla 274: Consultas de usuarios, reglas de procesamiento de eventos e informes 315
Captura de pantalla 275: Definir restricciones: Editar una restricción de consulta 316

Captura de pantalla 276: Definir restricciones: Personalizar la condición 317
Captura de pantalla 277: Reglas del firewall en Microsoft® Windows® XP 340
Captura de pantalla 278: Ventana de política de seguridad local 341
Captura de pantalla 279: Auditar propiedades de acceso a objetos 342
Captura de pantalla 280: Programas admitidos en Microsoft® Windows® Vista o una versión posterior 343
Captura de pantalla 281: Ventana de política de seguridad local 344
Captura de pantalla 282: Auditar propiedades de acceso a objetos 345
Captura de pantalla 283: Activar reglas del firewall en Microsoft® Windows® Server 2003 346
Captura de pantalla 284: Reglas del firewall en Microsoft®Windows® Server 2008 347
Captura de pantalla 285: Consola de política de dominio en Microsoft® Windows® Server 2003 348
Captura de pantalla 286: Administración de políticas de grupo en Microsoft® Windows® Server 2008 R2 349
Captura de pantalla 287: Editor de administración de políticas de grupo 350
Captura de pantalla 288: Reglas predefinidas 351
Captura de pantalla 289: Desactivar UAC 352
Captura de pantalla 290: Seleccione el modo de recopilación de datos 354
Captura de pantalla 291: Solucionador de problemas de comprobaciones automáticas 355
Captura de pantalla 292: Solucionador de problemas de corrección automática de problemas detectados 355
Captura de pantalla 293: Si el problema persiste, busque artículos en nuestra base de conocimiento. 356
Captura de pantalla 294: Comprobar problemas manualmente 356
Captura de pantalla 295: Especificar detalles de contacto 357
Captura de pantalla 296: Escribir la descripción del problema y otros datos 357
Captura de pantalla 297: Recopilar información de la máquina 358
Captura de pantalla 298: Finalizar el proceso de resolución de problemas 358

Lista de tablas

Tabla 1: Motores de GFI EventsManager 24
Tabla 2: Términos y convenciones que se usan en este manual 25
Tabla 3: Dispositivos admitidos por GFI EventsManager 28
Tabla 4: Beneficios de la instalación de GFI EventsManager en una DMZ 30
Tabla 5: Requisitos de hardware 32
Tabla 6: Requisitos de espacio de almacenamiento 33
Tabla 7: Puertos y protocolos del firewall 33
Tabla 8: Permisos del firewall 34
Tabla 9: Configuración de orígenes de eventos 35
Tabla 10: Actualizar GFI EventsManager 36
Tabla 11: Componentes instalados mediante EventsManager.exe 45
Tabla 12: Opciones de la consola de inicio rápido 54
Tabla 13: Opciones de la consola de inicio rápido 56
Tabla 14: Agregar nuevos orígenes de eventos manualmente 61
Tabla 15: Agregar nuevos orígenes de eventos manualmente 70
Tabla 16: Ficha Synchronization properties - General 71
Tabla 17: Opciones de grupo de orígenes de eventos 74
Tabla 18: Propiedades de orígenes de eventos - Opciones generales 76
Tabla 19: Tipos de licencia 78
Tabla 20: Opciones de supervisión de orígenes de eventos 82
Tabla 21: Grupo de base de datos de Microsoft® SQL: General 84
Tabla 22: Grupo de base de datos de Microsoft® SQL: Credenciales de inicio de sesión 85
Tabla 23: Grupo de base de datos de Microsoft® SQL - SQL Server® Auditoría 87
Tabla 24: Grupo de base de datos de Microsoft® SQL - Configuración 88
Tabla 25: Base de datos de Microsoft® SQL - Opciones de la ficha General 90
Tabla 26: Base de datos de Microsoft® SQL - Ficha Connection Settings 91
Tabla 27: Base de datos de Microsoft® SQL - Opciones de la ficha Settings 92
Tabla 28: Auditorías admitidas por Oracle Server 92
Tabla 29: Etapas de configuración de Oracle Server 93
Tabla 30: Grupo de base de datos de Oracle- General 94
Tabla 31: Grupo de base de datos de Oracle Database - Auditoría de Oracle 97
Tabla 32: Ficha Oracle Server properties - General 99
Tabla 33: Ficha Oracle Server properties - Connection Settings 100
Tabla 34: Ficha Oracle Server properties - Audit by Objects 101
Tabla 35: Ficha Oracle Server properties - Audit by Statements 102
Tabla 36: Registro de eventos de Windows® recopilados por GFI EventsManager 103
Tabla 37: Información recopilada por GFI LanGuard 119
Tabla 38: Dispositivos compatibles con GFI EndPointSecurity 124

Tabla 39: Desplazarse en el Explorador de eventos 127
Tabla 40: Explorador de eventos: Crear nuevo informe 129
Tabla 41: Explorador de eventos: Crear una nueva vista 131
Tabla 42: Descripción de las posiciones del panel 134
Tabla 43: Supervisión de estado: Secciones de vista general 138
Tabla 44: Supervisión de estado: Vista de actividad de tareas 142
Tabla 45: Supervisión de estado: Vista de estadísticas 143
Tabla 46: Desplazarse por la ficha Reporting 146
Tabla 47: Informes disponibles 147
Tabla 48: Crear carpeta de informes: Opciones de programación 150
Tabla 49: Opciones de patrón de rango 156
Tabla 50: Configuración de registro del informe 157
Tabla 51: Opciones de patrón de rango 162
Tabla 52: Configuración de registro del informe 163
Tabla 53: Descripción del resumen diario por correo electrónico 167
Tabla 54: Información de encabezado del informe de configuración 167
Tabla 55: Información de encabezado del informe de reglas 169
Tabla 56: Descripción del informe del historial operativo 170
Tabla 57: Opciones de exportación del historial operativo 171
Tabla 58: Encabezados de los informes generales de actividad 172
Tabla 59: Opciones de exportación del historial operativo 173
Tabla 60: Analizar informes: Herramientas 174
Tabla 61: Opciones para agregar definiciones de columna 175
Tabla 62: Plantillas HTML predeterminadas 177
Tabla 63: Plantilla HTML: Secciones editables 178
Tabla 64: Marcadores de plantilla de informes HTML 178
Tabla 65: Carpetas de conjuntos de reglas comunes disponibles 182
Tabla 66: Configurar nuevas reglas de procesamiento de eventos: Acciones 188
Tabla 67: Acciones disponibles de reglas de procesamiento de eventos 193
Tabla 68: Parámetros de filtrado de eventos de Windows®: Campo Event ID 194
Tabla 69: Parámetros de filtrado de eventos de Windows®: Campos Source, Category y User 194
Tabla 70: Parámetros de filtrado de syslog: Campos Message y Process 194
Tabla 71: Comprobaciones de supervisión - Eventos de acción 201
Tabla 72: Comprobaciones de supervisión - Eventos de acción 206
Tabla 73: Comprobaciones de supervisión - Eventos de acción 212
Tabla 74: Acciones de clasificación predeterminadas 217
Tabla 75: Cuadro de diálogo Alerting Options - Email alerts 220
Tabla 76: Cuadro de diálogo Alerting Options: SMS 222
Tabla 77: Opciones de alerta: Capturas SNMP 223
Tabla 78: Opciones de alerta: Configuración general 224

Tabla 79: Opciones de filtrado de usuarios 238
Tabla 80: Opciones de rotación de base de datos 261
Tabla 81: Configurar operaciones de base de datos 262
Tabla 82: Tipos de tareas de mantenimiento 263
Tabla 83: Crear tareas de mantenimiento - Opciones de programación 267
Tabla 84: Filtrar datos exportados 270
Tabla 85: Crear tareas de mantenimiento - Opciones de programación 271
Tabla 86: Operaciones de base de datos: Estructura del nombre del archivo de exportación 271
Tabla 87: Exportar a SQL: Opciones del servidor 274
Tabla 88: Filtrar datos de exportación 275
Tabla 89: Crear tareas de mantenimiento - Opciones de programación 276
Tabla 90: Filtrar datos exportados 279
Tabla 91: Crear tareas de mantenimiento - Opciones de programación 279
Tabla 92: Crear tareas de mantenimiento - Opciones de programación 282
Tabla 93: Exportar a SQL: Opciones del servidor 284
Tabla 94: Opciones de actualización automática 298
Tabla 95: Usos de restricciones de consulta 314
Tabla 96: Iniciar el cuadro de diálogo Edit Query Restrictions 315
Tabla 97: Definir restricciones: Operadores de campo 316
Tabla 98: Definir restricciones: Herramientas de condición de consulta 317
Tabla 99: Parámetros de /op:registerService 320
Tabla 100: /op:disable Parameter 320
Tabla 101: Parámetros /op:SetLicense 320
Tabla 102: Parámetros /op:configureAlerting 321
Tabla 103: Parámetro /op:setAdminEmail 321
Tabla 104: Parámetro /op:getComputers 322
Tabla 105: Parámetros /importFromSQL 323
Tabla 106: Parámetros /importFromDlib 323
Tabla 107: Parámetros /copyData 324
Tabla 108: Parámetros /importFromLegacyFile 326
Tabla 109: /exportToFile 326
Tabla 110: Parámetros /importFromFile 329
Tabla 111: Parámetros /commitDeletedRecords 330
Tabla 112: Parámetros /exportToSQL 330
Tabla 113: Parámetros /decryptDatabase 332
Tabla 114: Parámetros /encryptDatabase 332
Tabla 115: Parámetros /displayAllDLib 333
Tabla 116: /copyMoveDLib 333
Tabla 117: Parámetros de los informes de configuración 334
Tabla 118: Parámetros de informes de estado 335

Tabla 119: Parámetros de informes de eventos 336
Tabla 120: CMD: Parámetros de ImportSettings.exe 337
Tabla 121: CMD: Parámetros ExportSettings.exe 338

1 Introducción

El considerable volumen de registros de eventos del sistema generado por día es de creciente importancia para las organizaciones que deben registrar la información con fines forenses y de cumplimiento. Es esencial llevar a cabo una supervisión de los registros de eventos de toda la red en tiempo real, ejecutar análisis y generar informes para abordar los incidentes y los problemas de seguridad, además de combatir los riesgos relacionados con la continuidad de la empresa.

GFI EventsManager asiste en esta tarea monumental al supervisar y administrar los registros de eventos de forma centralizada y automática; además, admite una amplia diversidad de tipos de eventos generados por aplicaciones y dispositivos de los principales proveedores, y por aplicaciones y dispositivos personalizados.

En este capítulo, se proporciona información acerca de cómo se logra la administración de eventos utilizando GFI EventsManager.

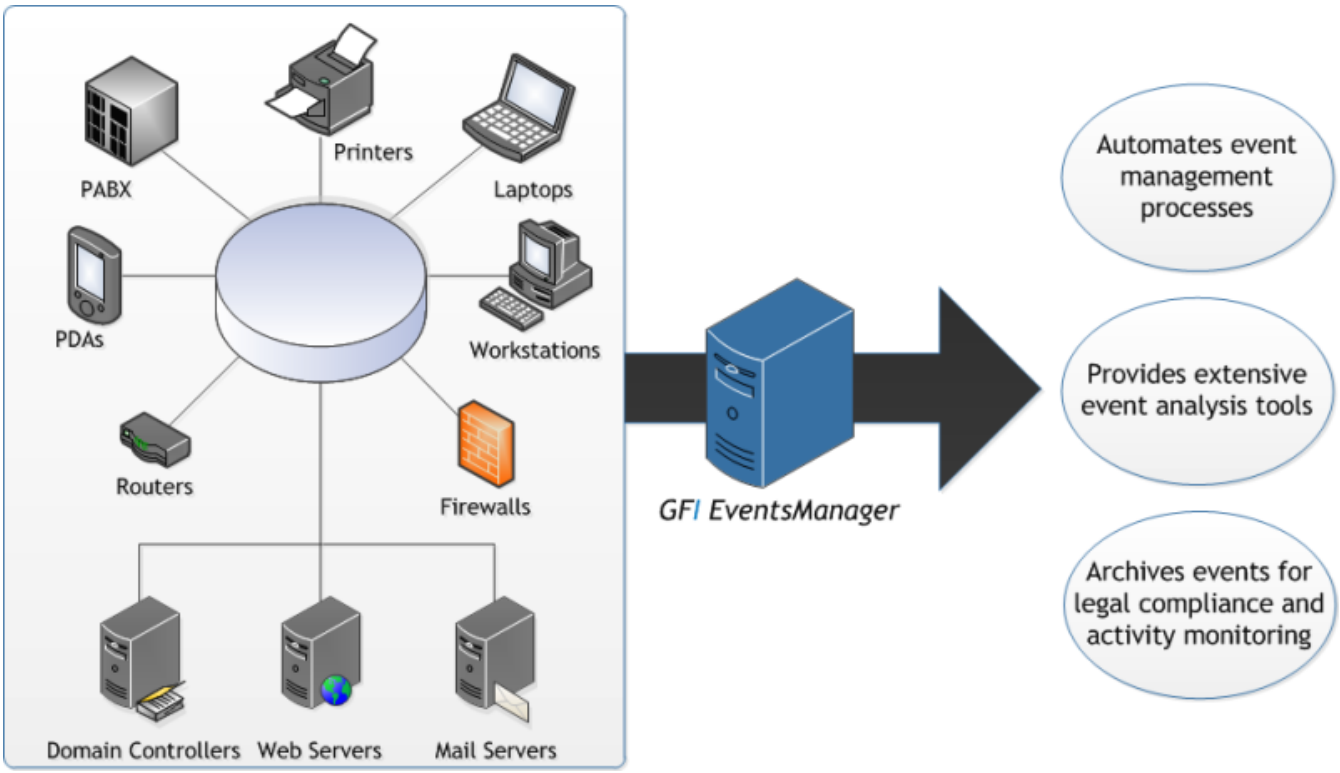
Temas de este capítulo:

1.1 Acerca de GFI EventsManager 21

1.2 Cómo funciona GFI EventsManager 23

1.3 Convenciones utilizadas en esta guía 25

1.1 Acerca de GFI EventsManager



Captura de pantalla 1: GFI EventsManager se integra en cualquier infraestructura de TI existente

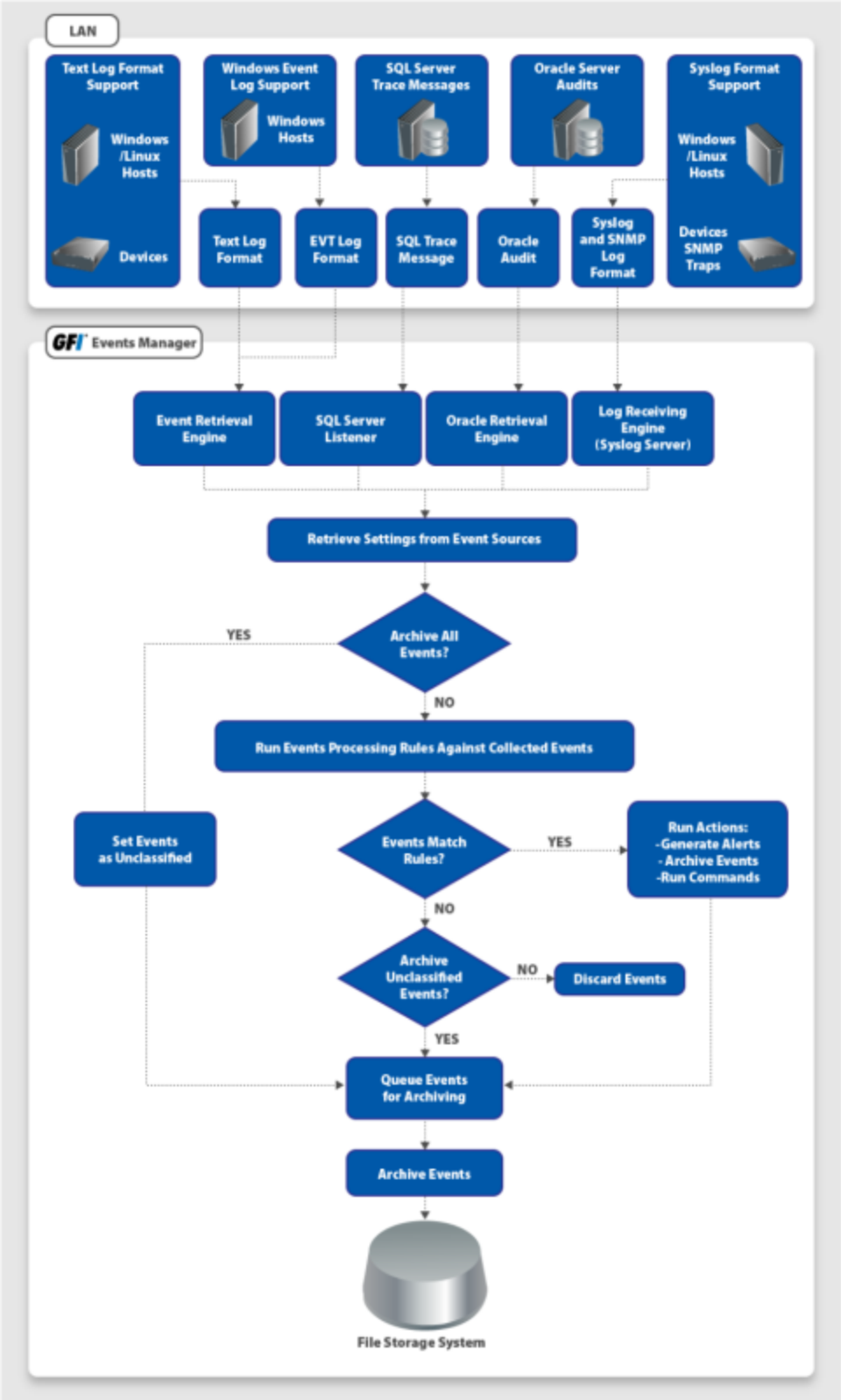
GFI EventsManager es una solución de administración de registros de eventos orientada a los resultados que se integra en cualquier infraestructura de TI existente, y automatiza y simplifica las tareas relacionadas con la administración de eventos de toda la red.

A través de las funciones admitidas por GFI EventsManager, usted puede:

- Supervisar automáticamente los equipos y dispositivos de red a través del amplio rango de soporte de registro de eventos de GFI EventsManager', como registros de texto, registros de eventos de Windows®, Syslogs, capturas SNMP, eventos de supervisión activa e incluso registros de eventos personalizados
- Supervisar los equipos y servicios que se ejecutan en la red a través de funciones de supervisión activas, como la comprobación continua de la disponibilidad de sitios HTTP/HTTPS/FTP, consultas de roles de servidor, consultas de firewall y más
- Optimizar la seguridad y el rendimiento a la vez que realiza el seguimiento de problemas operativos al auditar los sistemas/dispositivos críticos, como enrutadores, firewalls, sensores, servidores y motores de bases de datos
- Crear y mantener un sistema de seguridad de red automatizado que detecte ataques de intrusión
- Lograr el cumplimiento de diversas normas y leyes, como SOX, PCI DSS, Código de Conexión, HIPAA, leyes de protección de datos y otras
- Detectar proactivamente eventos que generarán un desastre, como un error de hardware. Cuando se procesan estos eventos, GFI EventsManager proporciona una advertencia oportuna para brindarle el control y tomar medidas correctivas
- Minimizar el riesgo y la pérdida de ganancia debido al tiempo de inactividad y la configuración incorrecta de los sistemas
- Buscar con facilidad eventos desde cualquier cantidad de bases de datos a través del Explorador de eventos, que lo ayuda a llevar a cabo investigaciones forenses con mínima intervención humana
- Procesar y archivar automáticamente los registros de eventos, recopilar y destacar la información que usted necesita saber acerca de los eventos más importantes que se producen en la red para que nunca lo sorprendan
- Generar nivel técnico de TI e informes de nivel gerencial a partir de la extensa lista de informes y crear otros nuevos informes a partir de los informes existentes o los eventos recopilados
- Proteger su empresa mediante el seguimiento de los eventos de seguridad en su red. Descubrir quién es responsable de las infracciones de seguridad y amenazas de la red

Para obtener una lista completa de las características, consulte:
http://www.gfi.com/eventsmanager#features

1.2 Cómo funciona GFI EventsManager



Captura de pantalla 2: Las etapas operativas de GFI EventsManager

La funcionalidad operativa de GFI EventsManager se divide en las siguientes etapas:

- Etapa 1: Recopilación de eventos
- Etapa 2: Procesamiento de eventos

1.2.1 Etapa 1: Recopilación de eventos

Durante la etapa de recopilación de eventos, GFI EventsManager recopila registros de orígenes de eventos específicos. Esto se logra mediante el uso de dos motores de recopilación de eventos: el **motor de recuperación de eventos** y el **motor de recepción de eventos**.

Tabla 1: Motores de GFI EventsManager

Motor	Descripción
El motor de recuperación de eventos	Se utiliza para recopilar los registros de eventos y registros de texto de Windows® a partir de orígenes de eventos en red. Durante el proceso de recopilación de eventos, este motor hará lo siguiente: 1. Iniciar sesión en el origen del evento 2. Recopilar eventos del origen 3. Enviar los eventos recopilados al servidor de GFI EventsManager 4. Desconectarse del origen del evento El motor de recuperación de eventos recopila eventos a intervalos de tiempo específicos. El intervalo de recopilación de eventos se puede configurar en la Consola de administración de GFI EventsManager.
El agente de escucha SQL Server®	El agente de escucha recibe mensajes de seguimiento del Microsoft® SQL Server® analizado en tiempo real. Tras la recepción, GFI EventsManager procesa el mensaje inmediatamente.
El motor de recuperación de Oracle	El motor de recuperación de Oracle se conecta periódicamente a los servidores de Oracle y recopila las auditorías de una tabla de auditoría específica. Al igual que el motor de recuperación de eventos de Microsoft® Windows®, GFI EventsManager procesa los eventos generados por el servidor de Oracle.
Motor de recepción de registros	El motor de recepción de eventos funciona como un servidor de Syslog y captura SNMP; escucha y recopila eventos/mensajes Syslog y capturas SNMP enviados por varios orígenes en la red. A diferencia del motor de recuperación del evento, el motor de recepción de eventos recibe mensajes directamente desde el origen del evento, por lo que no requiere que inicie sesión de forma remota en los orígenes de eventos para la recopilación de eventos. Además, los eventos/mensajes de Syslog y captura SNMP se recopilan en tiempo real y, por lo tanto, no hace falta configurar intervalos de tiempo de recopilación. De forma predeterminada, el motor de recepción de eventos escucha los mensajes Syslog en el puerto 514 y, para mensajes de captura SNMP, en el puerto 162. Ambas configuraciones de los puertos son, sin embargo, personalizables a través de la Consola de administración de GFI EventsManager.

1.2.2 Etapa 2: Procesamiento de eventos

Durante esta etapa, GFI EventsManager ejecuta un conjunto de reglas de procesamiento de eventos contra los eventos recopilados. Las reglas de procesamiento de eventos son instrucciones que:

- Analizan los registros recopilados y clasifican los eventos procesados en un nivel de importancia crítica, alta, media, baja y ruido (eventos no deseados o repetidos)
- Filtran eventos que responden a condiciones específicas
- Activan alertas por correo electrónico, SMS y red en eventos clave
- Activan acciones de corrección, como la ejecución de archivos ejecutables o secuencias de comandos, en eventos clave
- Opcionalmente, archivan eventos recopilados en el back-end de base de datos

GFI EventsManager se puede configurar para archivar eventos sin tener que ejecutar reglas de procesamiento de eventos. En tales casos, a pesar de que no se apliquen reglas contra registros recopilados, el archivo todavía se controla en la etapa de procesamiento de eventos. Para obtener más información, consulte Reglas de procesamiento de eventos.

Importante

Algunos de los módulos clave en GFI EventsManager se deben ejecutar con privilegios administrativos. Para obtener más información sobre estos módulos consulte el siguiente artículo: http://go.gfi.com/?pageid=esm_process_rights.

1.3 Convenciones utilizadas en esta guía

En la tabla siguiente, se describen los términos y las convenciones comunes utilizados en esta Guía:

Tabla 2: Términos y convenciones que se usan en este manual

Término	Descripción
	Información adicional y referencias esenciales para la operación de GFI EventsManager.
	Notificaciones y precauciones importantes sobre los problemas comunes que pueden surgir.
>	Instrucciones de navegación paso a paso para acceder a una función concreta.
Texto en negrita	Elementos que se seleccionan, como nodos, opciones de menú o botones de comando.
Texto en cursiva	Parámetros y valores que debe reemplazar por valores por el valor aplicable, como rutas de acceso y nombres de archivo personalizados.
`Código`	Indica los valores de texto que se escriben, como comandos y direcciones.

2 Instalación de GFI EventsManager

En este capítulo, se describen los posibles escenarios de implementación admitidos por GFI EventsManager. Es indispensable revisar los requisitos del sistema y la configuración del equipo antes de instalar el producto para garantizar la plena comunicación entre GFI EventsManager y los dispositivos/equipos de red que deben ser supervisados.

Temas de este capítulo:

2.1 Escenario de implementación 26

2.2 Requisitos del sistema 32

2.3 Actualizar GFI EventsManager 36

2.4 Instalar una nueva instancia de GFI EventsManager 45

2.5 Probar la instalación 54

2.1 Escenario de implementación

GFI EventsManager se puede instalar en cualquier equipo que cumpla los requisitos mínimos del sistema, independientemente de la ubicación en su red. Si desea recopilar registros de eventos de Microsoft®Windows® Vista o de sistemas operativos posteriores, se debe instalar GFI EventsManager en un equipo con Microsoft®Windows® Vista, 7, Server 2008 o Server 2012.

Utilice GFI EventsManager para administrar los registros de eventos que genera:

- El mismo equipo donde está instalado
- Todos los servidores, estaciones de trabajo y dispositivos de red a los que se puede obtener acceso desde el equipo en el que está instalado.

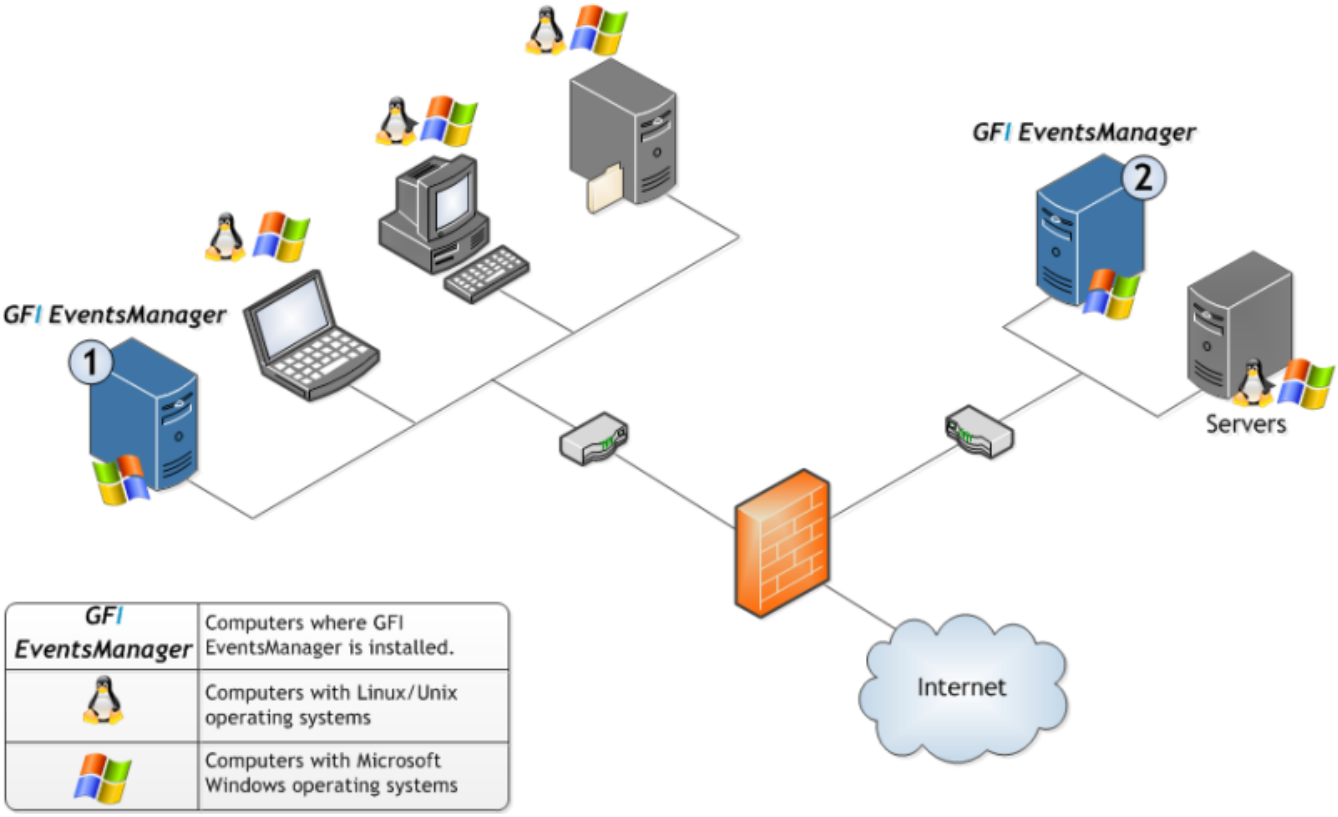


Figura 1: Escenario de implementación de GFI EventsManager

Esta sección contiene información acerca de la implementación de GFI EventsManager en una:

- Red de área local (LAN): supervisa la actividad de la red de producción, servidores y estaciones de trabajo principales
- Zona Desmilitarizada (DMZ): supervisa los eventos que generaron los servidores públicos, como los servidores de correo, los servidores web y los servidores DNS
- Red de área extensa (WAN): supervisa los eventos que generaron los equipos y dispositivos de red distribuidos en diferentes ubicaciones geográficas

2.1.1 GFI EventsManager en una Red de área local (LAN)

GFI EventsManager se puede implementar en redes basadas en Windows®, así como en entornos mixtos donde también se estén utilizando los sistemas Linux y Unix.

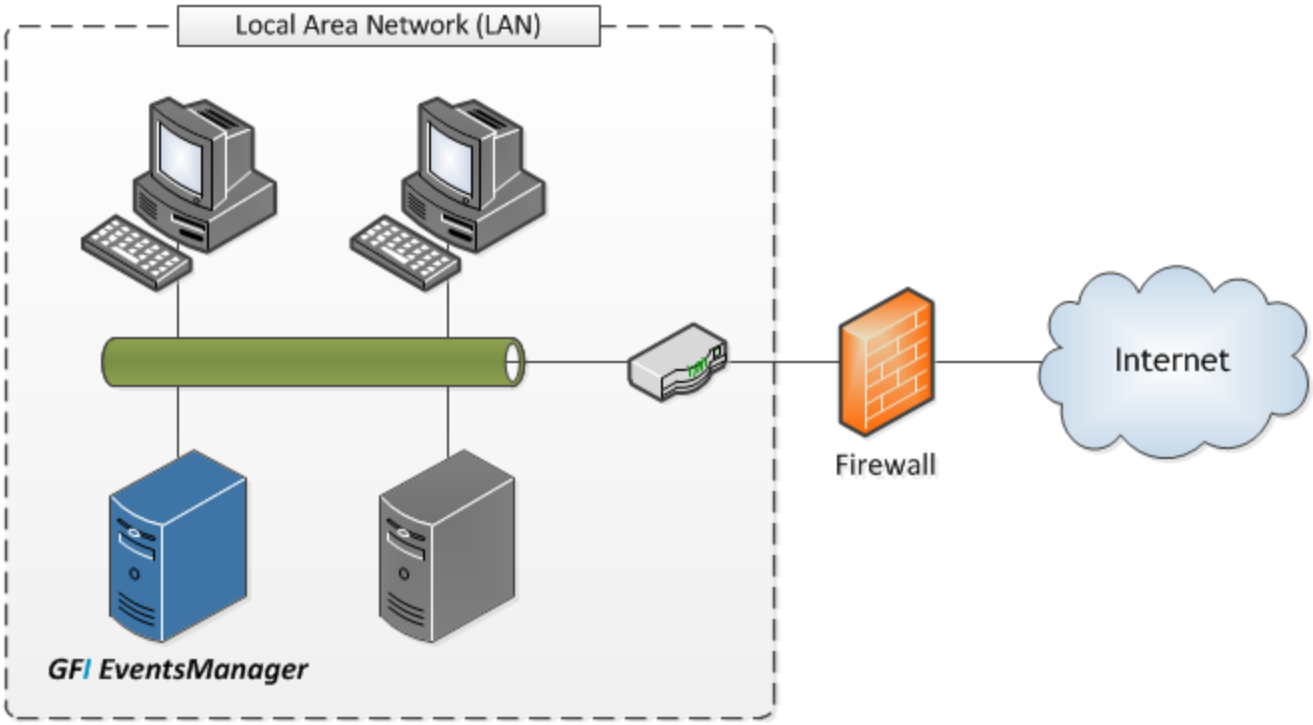


Figura 2: Implementar GFI EventsManager en una LAN

Cuando se instala en una red de área local (LAN), GFI EventsManager puede administrar eventos de Windows®, registros de texto, mensajes de syslog, capturas SNMP y auditorías de SQL Server® generados por cualquier hardware o software que se conecte a la LAN, incluidos:

Tabla 3: Dispositivos admitidos por GFI EventsManager

Dispositivo	Ejemplo
Estaciones de trabajo y equipos portátiles	Equipos y sistemas del usuario final
Servidores	Servidores web, servidores de correo, servidores DNS y más
Dispositivos de red	Enrutadores, conmutadores y cualquier otro dispositivo que genere registros de rendimiento
Software	Incluso GFI EndPointSecurity, GFI LanGuard y otras aplicaciones que generan registros
Servicios especializados	Servidor de Información de Internet de Microsoft® - IIS.
PABX, sistemas de acceso sin clave, sistemas de detección de intrusión y más	GFI EventsManager le permite supervisar cualquier dispositivo que esté conectado a la red.

2.1.2 GFI EventsManager en una zona desmilitarizada (DMZ)

GFI EventsManager puede supervisar los eventos generados por equipos en una DMZ, al instalarlo dentro de la LAN o directamente en la DMZ. Ya que, por lo general, un firewall o un enrutador protege esta zona con capacidades de filtrado de tráfico de red, debe asegurarse de que:

- Los puertos de comunicación utilizados por GFI EventsManager no estén bloqueados por el firewall. Para obtener más información sobre los puertos de comunicación utilizados por GFI EventsManager, consulte:http://go.gfi.com/?pageid=esm_ports.
- GFI EventsManager tiene privilegios administrativos sobre los equipos que se ejecutan en la DMZ.

Importante

GFI recomienda instalar GFI EventsManager directamente en la DMZ en lugar de habilitar puertos y permisos de firewall para habilitar la comunicación entre equipos, servidores y dispositivos de red LAN y DMZ.

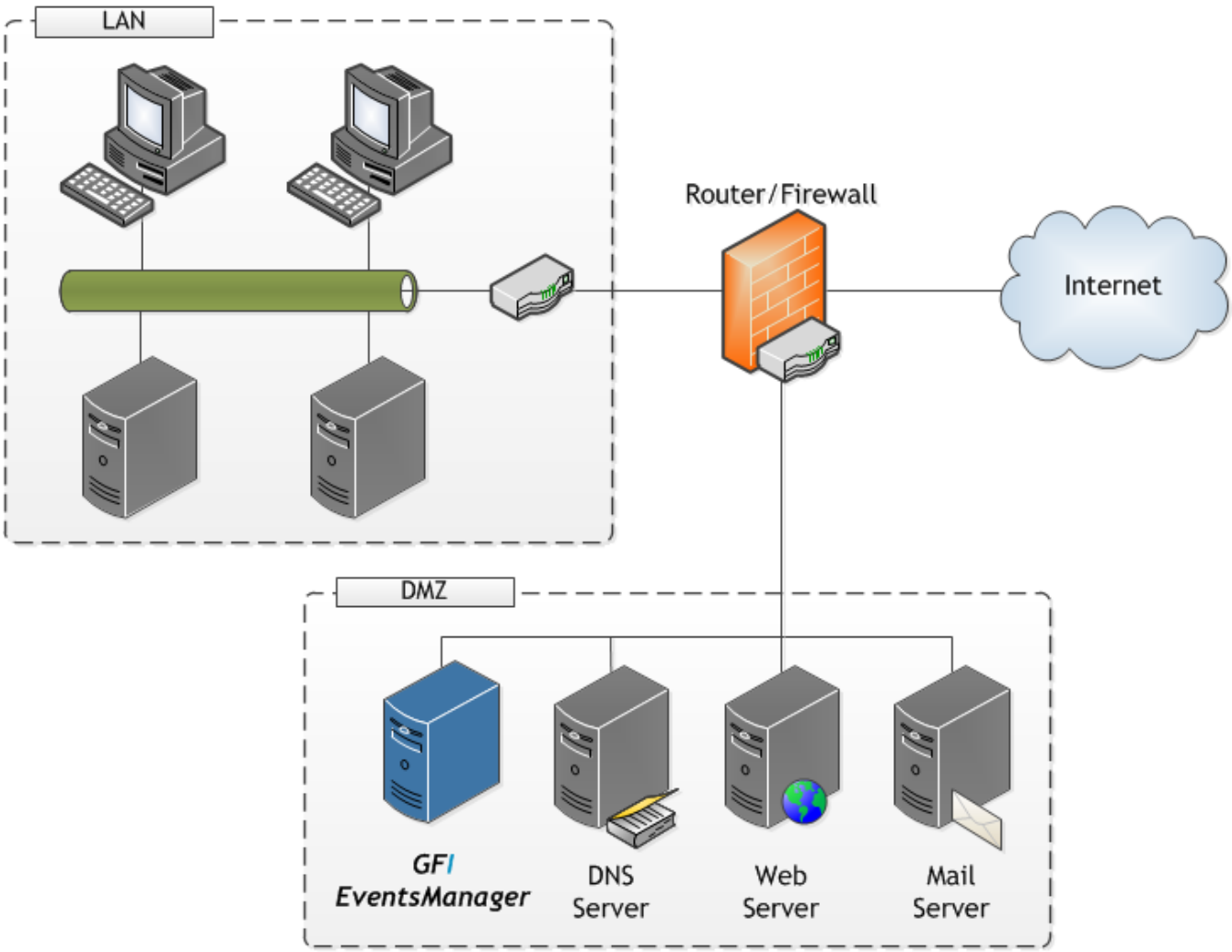


Figura 3: La DMZ se encuentra entre la LAN interna e Internet

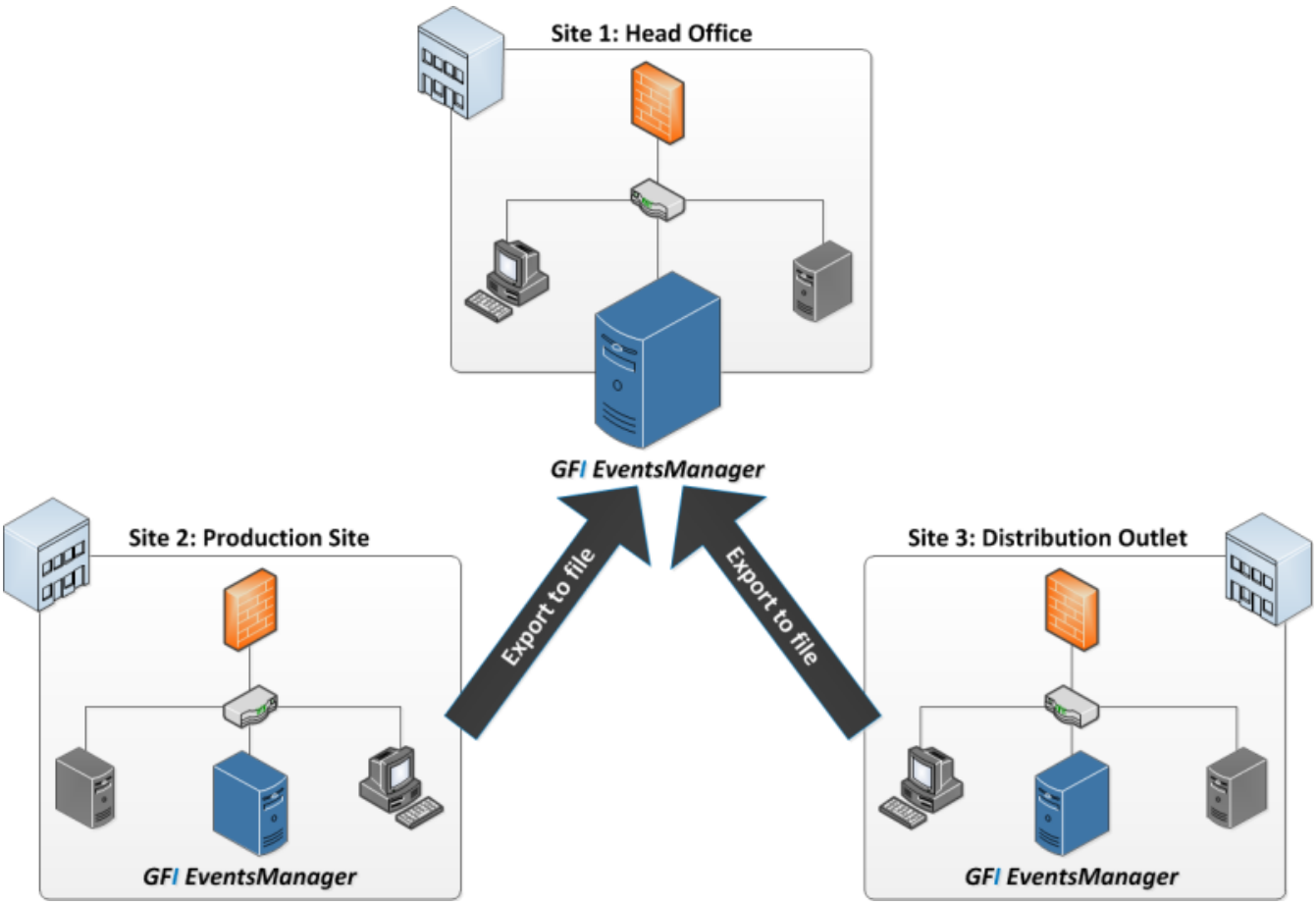
Una DMZ es la red neutral que se sitúa entre la red corporativa "interna" y el "mundo exterior" (Internet). La implementación de GFI EventsManager en una DMZ ayuda a automatizar la administración de los eventos generados por los sistemas de hardware y software DMZ, tales como:

Tabla 4: Beneficios de la instalación de GFI EventsManager en una DMZ

Automatización de la DMZ	Descripción
Automatizar la administración de eventos del servidor web y de correo	Las redes DMZ normalmente se utilizan para ejecutar sistemas de hardware y software que tienen roles específicos de Internet, como servidores HTTP, servidores FTP y servidores de correo. Por lo tanto, se puede implementar GFI EventsManager para administrar automáticamente los eventos generados por: » Servidores web, incluidos los registros web W3C generados por los servidores web Apache en plataformas web LAMP » Servidores web basados en Windows®, incluidos los registros web W3C generados por los servidores Internet Information Services (IIS) de Microsoft® » Servidores de correo basados en Linux/Unix y Windows®, incluidos los mensajes de los servicios de auditoría Syslog generados por Sun Solaris v. 9 o posterior » Automatizar la administración de eventos del servidor DNS » Si usted tiene un servidor DNS público, hay una buena probabilidad de que esté ejecutando un servidor DNS en la DMZ. Por lo tanto, puede utilizar GFI EventsManager para recopilar y procesar automáticamente los eventos del servidor DNS, incluso aquellos almacenados en sus registros del servidor DNS de Windows®.
Automatizar la administración de eventos del servidor DNS	Si usted tiene un servidor DNS público, hay una buena probabilidad de que esté ejecutando un servidor DNS en la DMZ. Por lo tanto, puede utilizar GFI EventsManager para recopilar y procesar automáticamente los eventos del servidor DNS, incluso aquellos almacenados en sus registros del servidor DNS de Windows®.
Automatizar la administración de eventos de dispositivos de red	Los enrutadores y firewall son dos dispositivos de red que se encuentran comúnmente en una DMZ. Los enrutadores y firewall especializados (por ejemplo: enrutadores de la serie Cisco IOS) no solo ayudan a proteger su red interna, sino que proporcionan funciones especiales, como la Traducción de la dirección del puerto (PAT) que puede aumentar el rendimiento operativo de sus sistemas. Al implementar GFI EventsManager en su DMZ, puede recopilar los eventos generados por estos dispositivos de red. Por ejemplo, puede configurar GFI EventsManager para que funcione como un servidor Syslog y recopilar en tiempo real los mensajes Syslog generados por los enrutadores Cisco IOS.

2.1.3 GFI EventsManager en una red de área extensa (WAN)

GFI EventsManager se puede instalar en entornos que tienen múltiples sitios en diferentes ubicaciones geográficas.



Captura de pantalla 3: Exportar datos desde sitios remotos a la instancia principal de GFI EventsManager

Esto se consigue mediante la instalación de una instancia de GFI EventsManager en cada ubicación. Periódicamente (en base a una programación), puede exportar eventos desde los sitios remotos e importarlos a la base de datos central para la completa consolidación de los registros de eventos.

Los eventos del sitio remoto se pueden ver a continuación en el Explorador de eventos. Los informes con datos pertinentes a sitios remotos también se pueden generar utilizando los datos de la base de datos central. Utilice la opción Switch Database para ver o informar sobre los datos almacenados en bases de datos remotas.

Nota

Para obtener más información consulte Cambiar de bases de datos de almacenamiento de archivos.

Nota

Para obtener más información, consulte Mantenimiento de base de datos.

2.2 Requisitos del sistema

Para instalar GFI EventsManager, el equipo host debe cumplir con los requisitos del sistema que se especifican a continuación. Si tiene pensado administrar un gran número de orígenes de eventos en una red de alto tráfico, considere el uso de un equipo con mayores especificaciones del sistema. Consulte las siguientes secciones para obtener información acerca de:

- Requisitos de hardware
- Sistemas operativos admitidos (32 y 64 bits)
- Otros componentes de software
- Requisitos de almacenamiento
- Puertos y protocolos del firewall
- Permisos del firewall
- Configuración de orígenes de eventos
- Excepciones del antivirus
- Consideraciones de identificación de equipos
- Recopilar registros de eventos de equipos que ejecutan Microsoft® Vista o una versión posterior

2.2.1 Requisitos de hardware

La siguiente tabla contiene los requisitos de hardware para GFI EventsManager:

Tabla 5: Requisitos de hardware

Componente de hardware	Especificación
Procesador	2,5 GHz de dos núcleos o superior.
RAM	3 GB
Disco duro	10 GB de espacio libre

> **Nota**
>
> El tamaño del disco duro depende de su entorno, el tamaño especificado en los requisitos es el mínimo requerido para instalar y archivar eventos.

2.2.2 Sistemas operativos admitidos (32 y 64 bits)

GFI EventsManager se puede instalar en un equipo que esté ejecutando cualquiera de los siguientes sistemas operativos:

- Windows® Server 2012 - Foundation, Essentials, Standard o Datacenter
- Windows® Server 2008 - Standard o Enterprise
- Windows® Server 2008 R2 – Standard o Enterprise
- Windows® Server 2003 SP2 - Standard o Enterprise
- Windows® 8 - Standard, Professional o Enterprise
- Windows® 7 - Enterprise, Professional o Ultimate
- Windows® Vista SP1 - Enterprise, Business o Ultimate

- Windows® XP Professional SP3
- Windows® SBS 2008
- Windows® SBS 2003

> **Nota**
>
> GFI EventsManager no se puede instalar en instalaciones Server Core.

2.2.3 Otros componentes de software

Se recomienda instalar los siguientes componentes de software adicionales para garantizar la plena funcionalidad de GFI EventsManager:

- Microsoft® .NET framework 4.0
- Microsoft® Data Access Components (MDAC) 2.8 o posterior
- Un servidor de correo (cuando se requieren alertas por correo electrónico)

> **Nota**
>
> Microsoft® Data Access Components (MDAC) 2.8 se puede descargar desde http://go.gfi.com/?pageid=esm_mdac

2.2.4 Requisitos de almacenamiento

Los requisitos de almacenamiento a continuación están basados en el tamaño medio de un registro de eventos, que es de 535 bytes por evento. Las siguientes especificaciones indican el tamaño del disco duro requerido, que responde a las demandas de su infraestructura:

Tabla 6: Requisitos de espacio de almacenamiento

Espacio en disco duro	Número de eventos
Eventos almacenados por 1 Gb de espacio de almacenamiento	2 006 994
Eventos almacenados en 500 Gb de espacio de almacenamiento	1 003 497 032

2.2.5 Puertos y protocolos del firewall

La siguiente tabla contiene los puertos y protocolos que deben habilitarse en el firewall del host de GFI EventsManager:

Tabla 7: Puertos y protocolos del firewall

Puerto	Protocolos	Descripción
135	UDP y TCP	Los equipos de destino utilizan este puerto para publicar información sobre los puertos dinámicos disponibles. GFI EventsManager utiliza esta información para poder comunicarse con los equipos de destino.
139 y 445	UDP y TCP	GFI EventsManager lo utiliza para recuperar las descripciones del registro de eventos de las máquinas de destino.
162	UDP y TCP	GFI EventsManager lo utiliza para recibir capturas SNMP. Asegúrese de que este puerto esté abierto en el equipo donde está instalado GFI EventsManager.
514	UDP y TCP	GFI EventsManager lo utiliza para recibir mensajes Syslog.
1433	UDP y TCP	GFI EventsManager lo utiliza para comunicarse con el back-end de base de datos de SQL Server®. Asegúrese de que este puerto esté habilitado en Microsoft®SQL Server® y en el equipo donde esté instalado GFI EventsManager.

Puerto	Protocolos	Descripción
1521	UDP y TCP	Se utiliza para recopilar los registros de auditoría de Oracle Server. El puerto 1521 es el puerto predeterminado para esta conexión. Si el puerto se cambia manualmente en la configuración de Oracle Listener, ajuste la configuración del firewall según corresponda.
49153	UDP y TCP	Utilizado por GFI EventsManager para recopilar eventos de orígenes de eventos con Microsoft®Windows® Vista o Microsoft®Windows® 7.

2.2.6 Permisos del firewall

La siguiente tabla contiene los permisos que deben estar habilitados en el firewall del host de GFI EventsManager

Tabla 8: Permisos del firewall

Permisos del firewall y políticas de auditoría	Windows® Server 2008	Windows® Server 2003	Windows® XP	Windows® 7	Windows® Vista
Administración remota de registros de eventos	Habilitar	No corresponde	No corresponde	Habilitar	Habilitar
Uso compartido de archivos e impresoras	Habilitar	Habilitar	Habilitar	Habilitar	Habilitar
Detección de redes	Habilitar	No corresponde	No corresponde	Habilitar	Habilitar
Política de auditoría: Acceso a objetos	Habilitar	No corresponde	No corresponde	Habilitar	Habilitar
Política de auditoría: Seguimiento del proceso	Habilitar	No corresponde	No corresponde	Habilitar	Habilitar
Política de auditoría: Auditar administración de cuentas	Habilitar	Habilitar	Habilitar	Habilitar	Habilitar
Política de auditoría: Auditar eventos del sistema	Habilitar	Habilitar	Habilitar	Habilitar	Habilitar

Nota

Para obtener más información, consulte Habilitar permisos en orígenes de eventos manualmente o Habilitar permisos en orígenes de eventos automáticamente.

2.2.7 Configuración de orígenes de eventos

La siguiente tabla contiene los valores que se deben configurar en sus orígenes de eventos. Los orígenes de eventos son equipos que desea supervisar a través de GFI EventsManager:

Tabla 9: Configuración de orígenes de eventos

Tipo de registro	Descripción
Procesamiento de registros de eventos de Windows®	Habilite el registro remoto.
Procesamiento de registros de texto	Las carpetas de origen deben ser accesibles a través de recursos compartidos de Windows®.
Procesamiento de Syslog y capturas SNMP	Configure los orígenes/remitentes para enviar mensajes al equipo/dirección IP donde está instalado GFI EventsManager.
Análisis de equipos con Windows® Vista o posterior	Instale GFI EventsManager en un equipo con Windows® Vista o posterior.
Auditoría del sistema	Habilite la auditoría en los orígenes de eventos. Para obtener más información, consulte Habilitar permisos de orígenes de eventos de forma manual y Habilitar permisos de orígenes de eventos de forma automática.

2.2.8 Excepciones del antivirus

Si una aplicación antivirus está instalada en el equipo donde se está ejecutando GFI EventsManager, asegúrese de que:

- El tráfico no esté bloqueado en los puertos que usa GFI EventsManager
- **esmui.exe** y **esmproc.exe** tengan acceso permitido a través del firewall
- Las carpetas de GFI EventsManager se excluyan del análisis antivirus en tiempo real

2.2.9 Consideraciones de identificación de equipos

GFI EventsManager identifica los equipos a través del nombre de equipo o la dirección IP. Si se utilizan nombres de equipos compatibles con NETBIOS, asegúrese de que el servicio DNS esté configurado correctamente para la resolución del nombre. Una resolución de nombre poco fiable disminuye el rendimiento global del sistema. Si inhabilita NetBIOS sobre TCP/IP, puede seguir utilizando GFI EventsManager; sin embargo, debe especificar el nombre del equipo a través de su IP.

2.2.10 Recopilar registros de eventos desde equipos que ejecutan Microsoft® Vista o una versión posterior

GFI EventsManager no se puede instalar en Microsoft® Windows® XP para supervisar eventos de Microsoft® Windows® Vista o una versión posterior. Microsoft® Windows® Vista y Microsoft® Windows® 7 introdujeron grandes cambios estructurales en el registro de eventos y la administración del registro de eventos. Lo más importante de estos cambios:

- Un nuevo formato basado en XML para registros de eventos. Esto proporciona un enfoque más estructurado para informar sobre todos los sucesos del sistema.
- Categorización de eventos en cuatro grupos distintos: administrativos, operativos, analíticos y de depuración
- Un nuevo formato de archivo (EVTX), que reemplaza al antiguo formato de archivo EVT.

Debido a estos cambios, para recopilar y procesar registros de eventos de Microsoft® Windows® Vista o posterior, GFI EventsManager debe estar instalado en un sistema que ejecute:

- Windows® Vista
- Windows® 7
- Windows® Server 2008.

Nota

Los eventos de Windows® XP se pueden recopilar cuando se instala GFI EventsManager en Windows® Vista o máquinas posteriores.

Nota

Cuando GFI EventsManager está usando una cuenta que no pertenece al dominio para recopilar eventos de máquinas con Windows® Vista o una versión de Windows superior, las máquinas de destino deben tener inhabilitado el Control de cuentas de usuario (UAC). Para obtener más información, consulte Desactivar Control de cuentas de usuario (UAC).

2.3 Actualizar GFI EventsManager

La actualización desde versiones anteriores a GFI EventsManager 2011 no es totalmente compatible. Algunos parámetros pueden perderse debido a los cambios de la tecnología subyacente. GFI EventsManager se puede actualizar utilizando cualquiera de los métodos siguientes:

Tabla 10: Actualizar GFI EventsManager

Método	Descripción
Automáticamente	Inicie la nueva instalación y complete el asistente para actualizar y conservar los datos. Para obtener más información, consulte Actualizar desde una versión anterior.
Manualmente	Exporte las configuraciones y los eventos desde una versión anterior de GFI EventsManager e impórtelos en la nueva versión a través de las herramientas de importación/exportación y operaciones de la base de datos. Para obtener más información, consulte Crear tareas de mantenimiento e Importar y exportar configuraciones.

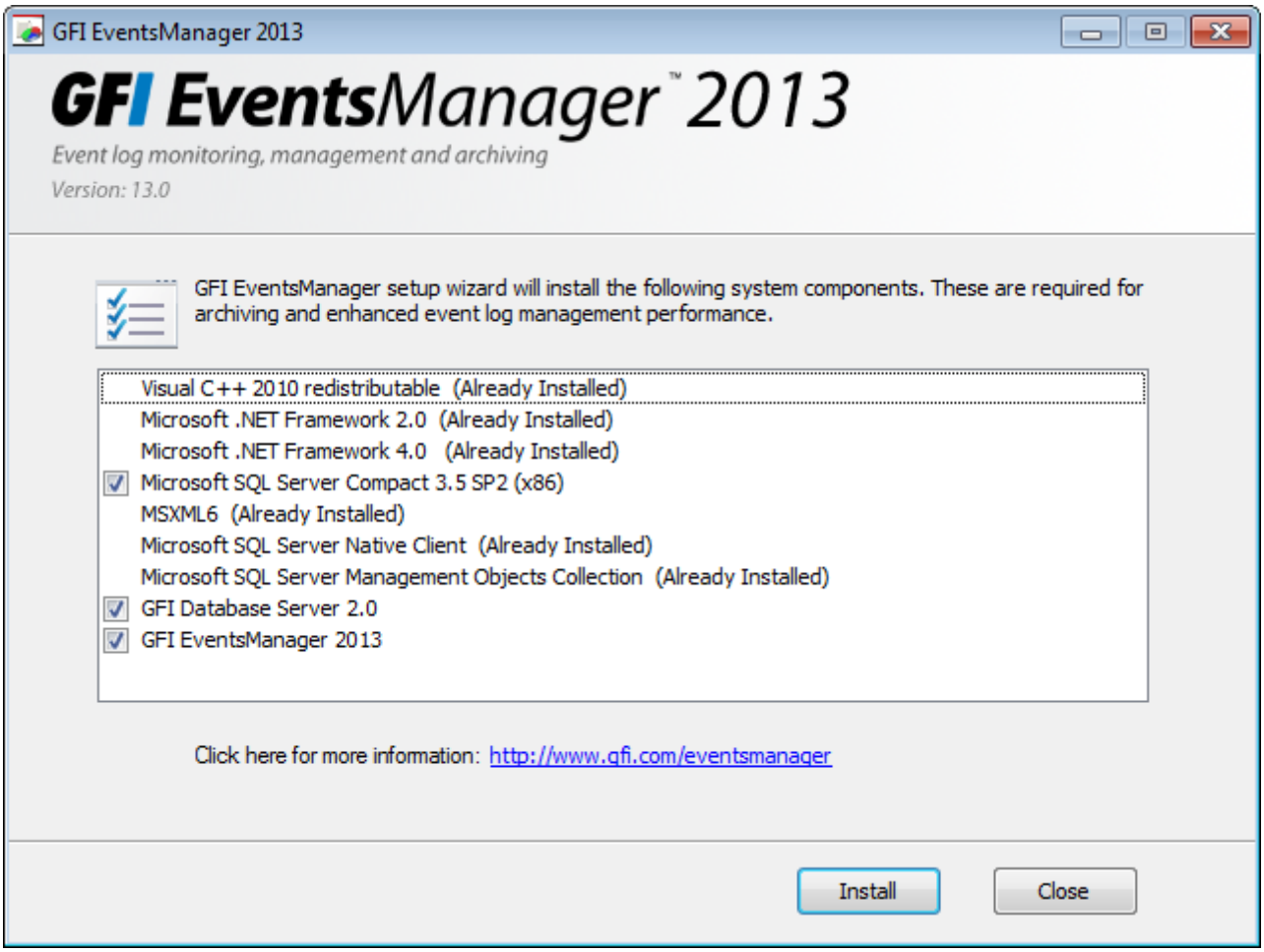
2.3.1 Actualizar desde una versión anterior

Nota

Antes de comenzar la actualización, inhabilite cualquier aplicación antivirus que se esté ejecutando en el sistema.

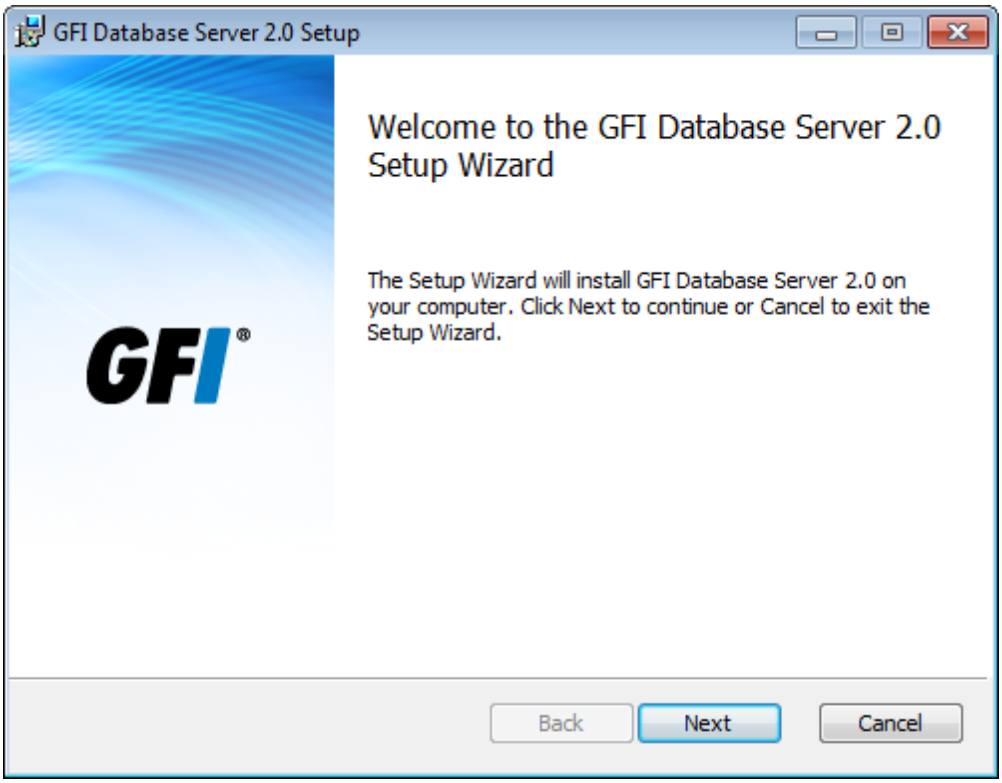
Para actualizar a una nueva versión:

1. Haga doble clic en **EventsManager.exe**.


GFI EventsManager 2013
GFI EventsManager 2013
Event log monitoring, management and archiving
Version: 13.0
GFI EventsManager setup wizard will install the following system components. These are required for archiving and enhanced event log management performance.
Visual C++ 2010 redistributable (Already Installed)
Microsoft .NET Framework 2.0 (Already Installed)
Microsoft .NET Framework 4.0 (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x86)
MSXML6 (Already Installed)
Microsoft SQL Server Native Client (Already Installed)
Microsoft SQL Server Management Objects Collection (Already Installed)
GFI Database Server 2.0
GFI EventsManager 2013
Click here for more information: http://www.gfi.com/eventsmanager
Install
Close

Captura de pantalla 4: Comprobación de requisitos previos a la actualización

2. El programa de instalación muestra una lista de componentes del sistema que deben instalarse antes de instalar el producto. Haga clic en **Install** para iniciar la instalación de los componentes del sistema que faltan (si es necesario).


GFI Database Server 2.0 Setup
Welcome to the GFI Database Server 2.0 Setup Wizard
The Setup Wizard will install GFI Database Server 2.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

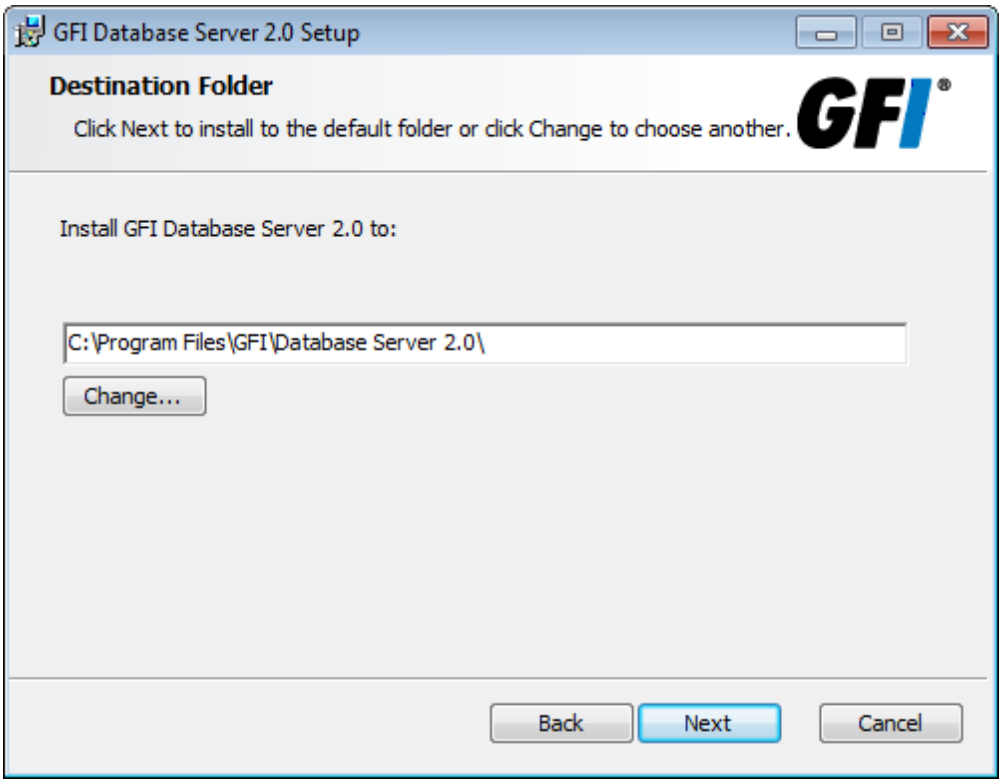
Captura de pantalla 5: Servidor de base de datos DLib

3. El asistente de instalación del servidor de base de datos DLib se abre automáticamente después de instalar los componentes del sistema. Haga clic en **Next** en la pantalla de bienvenida del asistente.

GFI Database Server 2.0 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI
GFI® End-User License Agreement
For: GFI FaxMaker®; GFI MailArchiver®, GFI MailEssentials® and GFI MailSecurity®; GFI WebMonitor®; GFI LanGuard®;
GFI Network Server Monitor®; GFI EventsManager®; GFI BackUp®; GFI Device Warden™ and GFI EndPointSecurity®
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

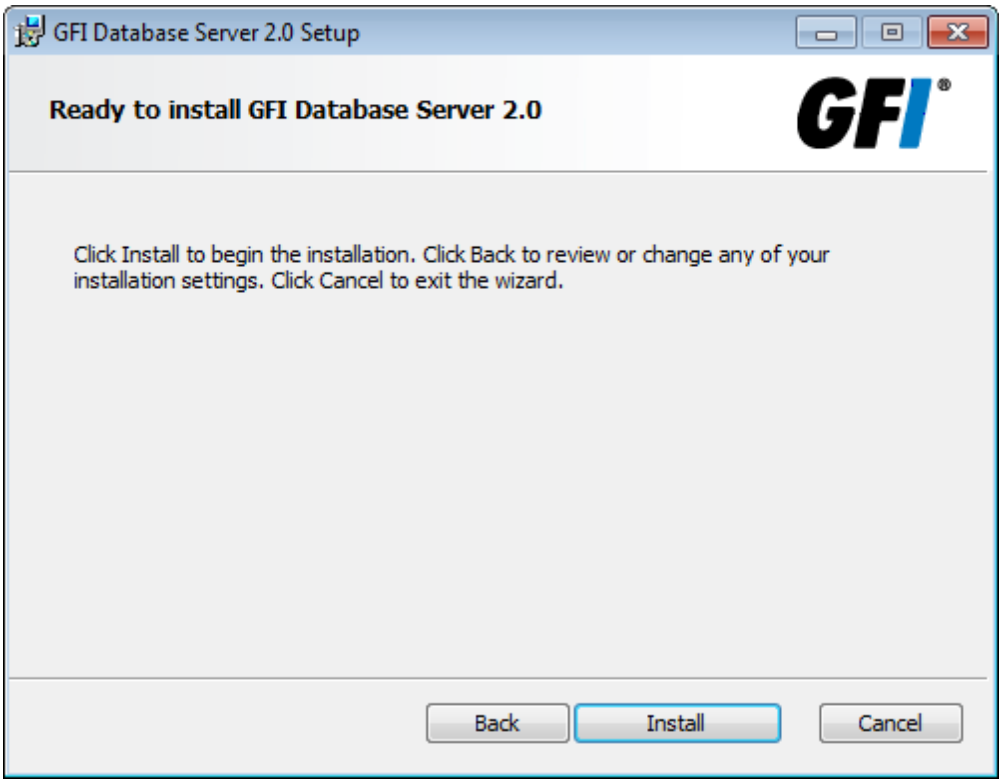
Captura de pantalla 6: EULA del servidor de base de datos DLib

4. Lea detenidamente el acuerdo de licencia. Seleccione **I accept the terms in the License Agreement** y haga clic en **Next**.



Captura de pantalla 7: Carpeta de instalación de DLib

5. Haga clic en **Next** para instalar el servidor de bases de datos en la carpeta predeterminada o haga clic en **Change...** para seleccionar una carpeta alternativa para la instalación.


GFI Database Server 2.0 Setup
Ready to install GFI Database Server 2.0
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Captura de pantalla 8: Iniciar instalación del servidor de base de datos DLib

6. Haga clic en **Install** para iniciar la instalación del servidor de base de datos DLib. Haga clic en **Finish** cuando se le solicite.

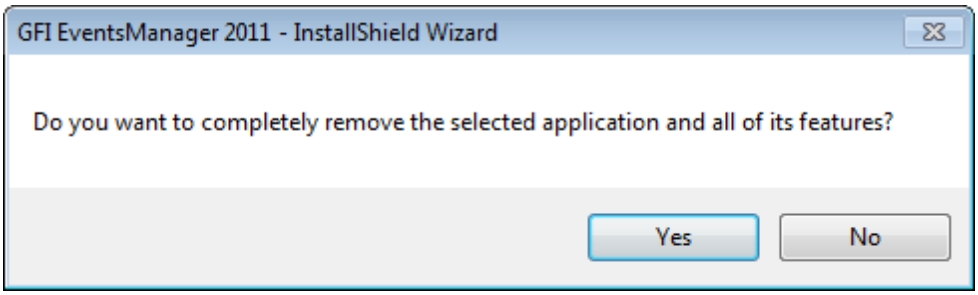
Nota

Una vez instalado el servidor de bases de datos, el instalador abre automáticamente el asistente de instalación de la Consola de administración de GFI EventsManager.

7. Haga clic en **Yes** para desinstalar la versión anterior de GFI EventsManager y continuar con la instalación de la nueva versión. Haga clic en **No** para detener la instalación.

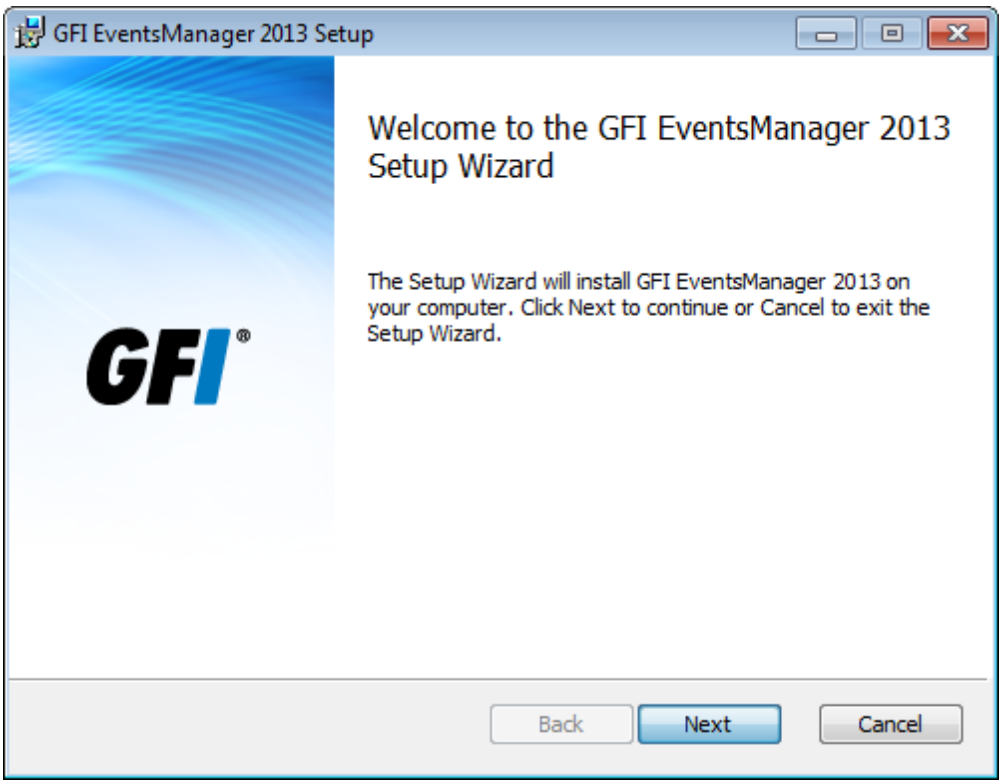
Nota

No es posible ejecutar dos instancias de la Consola de administración en el mismo equipo.


GFI EventsManager 2011 - InstallShield Wizard
Do you want to completely remove the selected application and all of its features?
Yes
No

Captura de pantalla 9: Eliminar archivos de la versión anterior

8. Haga clic en **Yes** para confirmar la eliminación de los archivos de la versión anterior de GFI EventsManager o haga clic en **No** para detener la instalación.


GFI EventsManager 2013 Setup
Welcome to the GFI EventsManager 2013 Setup Wizard
The Setup Wizard will install GFI EventsManager 2013 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

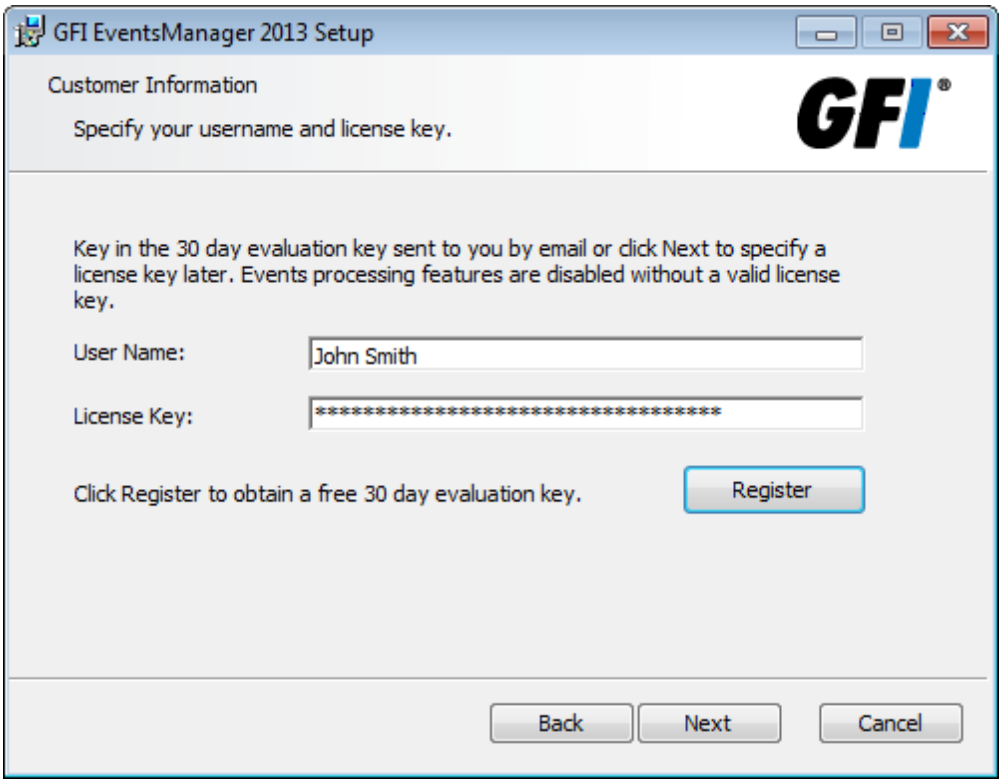
Captura de pantalla 10: Pantalla de bienvenida del asistente de instalación de GFI EventsManager

9. Haga clic en **Next** en la pantalla de bienvenida del asistente de instalación de GFI EventsManager.

GFI EventsManager 2013 Setup
End-User License Agreement
Carefully read the following end user license agreement
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™; GFI Device Warden™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

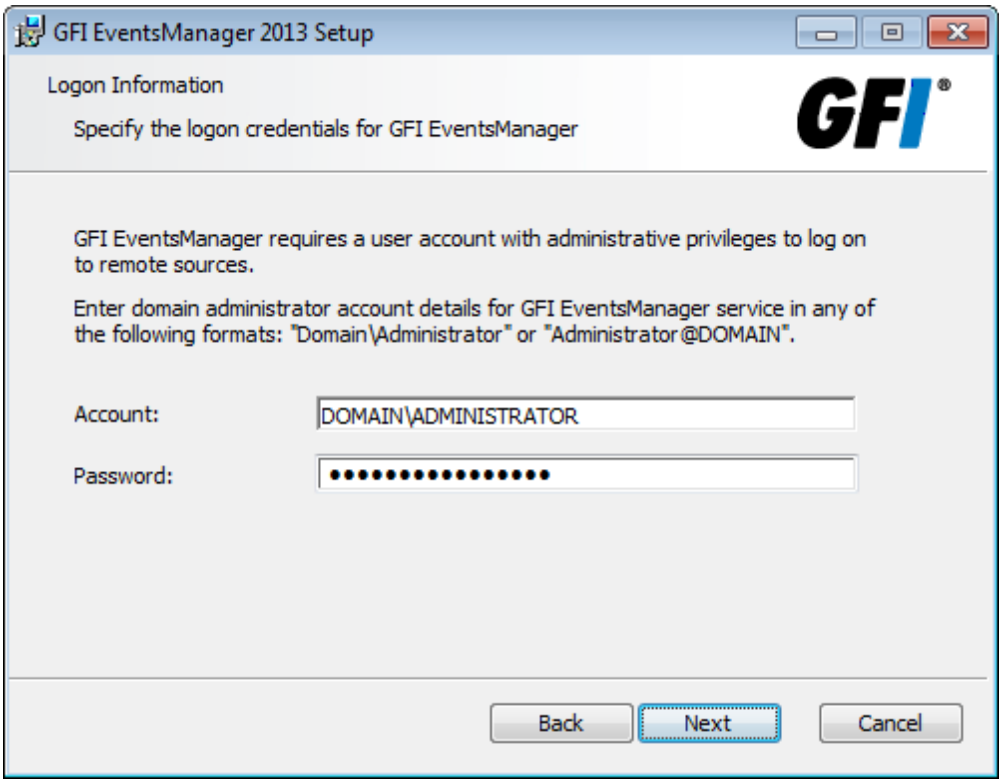
Captura de pantalla 11: EULA de GFI EventsManager

10. Lea detenidamente el acuerdo de licencia. Seleccione **I accept the terms in the License Agreement** y haga clic en **Next**.


GFI EventsManager 2013 Setup
Customer Information
Specify your username and license key.
Key in the 30 day evaluation key sent to you by email or click Next to specify a license key later. Events processing features are disabled without a valid license key.
User Name:
John Smith
License Key:
Click Register to obtain a free 30 day evaluation key.
Register
Back
Next
Cancel

Captura de pantalla 12: Detalles del registro de GFI EventsManager

11. Ingrese su nombre de usuario y la clave de licencia en los campos **User Name** y **License Key**. Para registrarse y acceder a una clave de licencia de evaluación gratuita de 30 días, haga clic en **Register**. Haga clic en **Siguiente**.

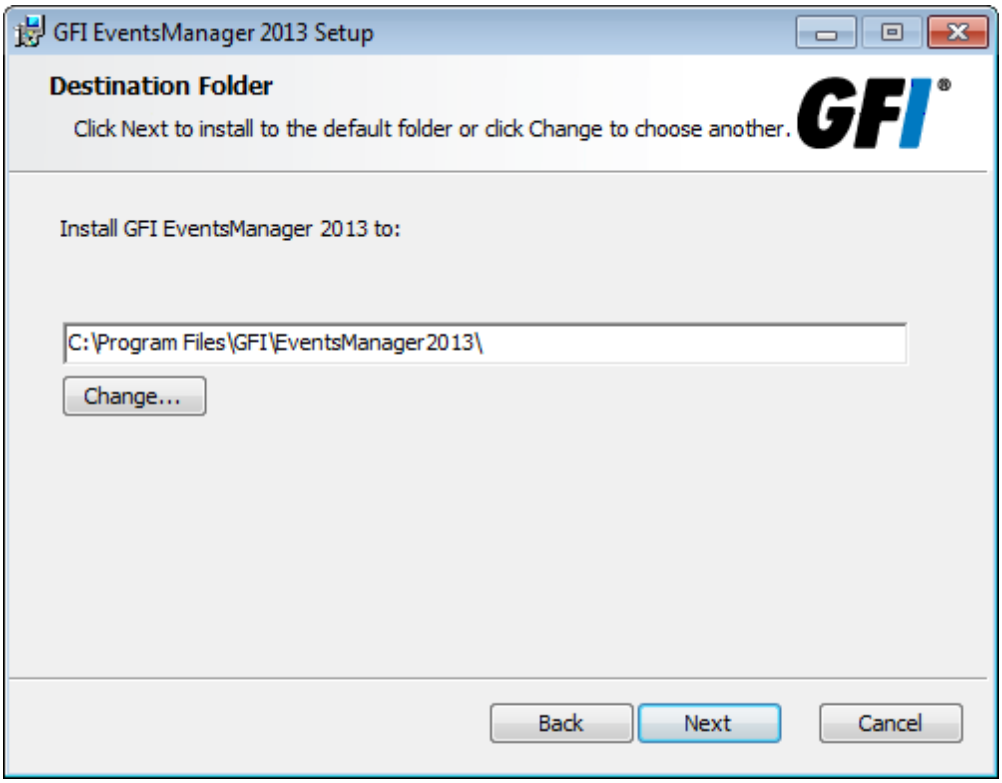

GFI EventsManager 2013 Setup
Logon Information
Specify the logon credentials for GFI EventsManager
GFI
GFI EventsManager requires a user account with administrative privileges to log on to remote sources.
Enter domain administrator account details for GFI EventsManager service in any of the following formats: "Domain\Administrator" or "Administrator@DOMAIN".
Account:
DOMAIN\ADMINISTRATOR
Password:
Back
Next
Cancel

Captura de pantalla 13: Credenciales de inicio de sesión remoto para supervisión de registros de eventos

12. Ingrese las credenciales de inicio de sesión que utiliza GFI EventsManager para iniciar sesión en equipos remotos.

Nota

Se recomienda usar un administrador de dominios o una cuenta con derechos administrativos sobre todos los equipos remotos administrados por GFI EventsManager.



Captura de pantalla 14: Carpeta de instalación de GFI EventsManager

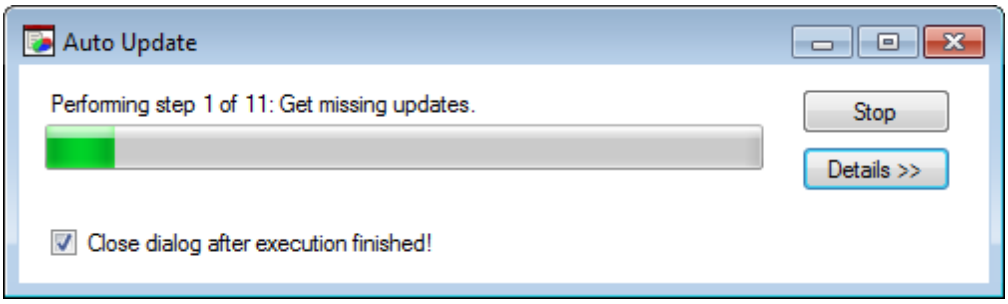
13. Haga clic en **Next** para instalar la Consola de administración en la carpeta predeterminada o haga clic en **Change...** para seleccionar una carpeta alternativa donde instalarla.

GFI EventsManager 2013 Setup
Ready to install GFI EventsManager 2013
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Captura de pantalla 15: Se completó la instalación de GFI EventsManager

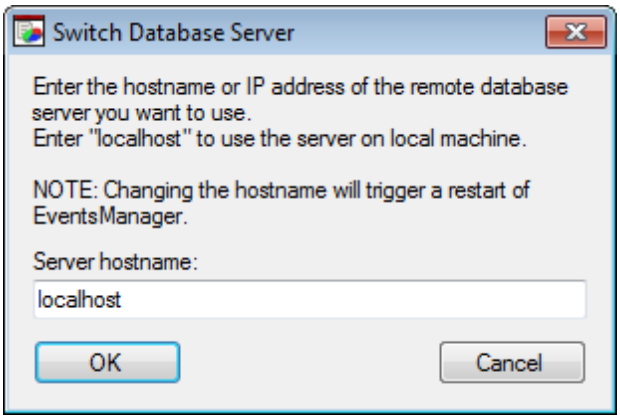
14. Haga clic en **Install** para iniciar la instalación.

15. Cuando la instalación se haya completado, haga clic en **Finish**.



Captura de pantalla 16: Comprobación automática de actualizaciones

16. Si GFI EventsManager detecta una conexión a Internet, automáticamente intenta descargar actualizaciones de productos de los servidores de actualización de GFI. Haga clic en **Details** para ampliar la sección de información del cuadro de diálogo Auto Update y ver las actualizaciones que se están descargando.


Switch Database Server
Enter the hostname or IP address of the remote database server you want to use.
Enter "localhost" to use the server on local machine.
NOTE: Changing the hostname will trigger a restart of EventsManager.
Server hostname:
localhost
OK
Cancel

Captura de pantalla 17: Definir el back-end de la base de datos

Nota

Después de aplicar las actualizaciones del producto, se abre el cuadro de diálogo **Switch Database Server**. Este cuadro de diálogo se usa para vincular la Consola de administración a un servidor de base de datos. Puede cambiar de servidor de bases de datos en la Consola de administración. Para obtener más información, consulte Cambiar de bases de datos de almacenamiento de archivos.

17. Especifique el equipo que tiene el servidor de bases de datos D-Lib instalado. Si la base de datos que desea usar está en:

- El host local, ingrese **localhost** (predeterminado)
- Un equipo remoto, ingrese el **nombre del equipo** o la **dirección IP**.

Haga clic en **OK** para aceptar.

Nota

Una vez completada la instalación, la Consola de administración se abre automáticamente. Para ejecutarla manualmente, haga clic en **Inicio > Todos los programas > GFI EventsManager > Management Console**.

Nota

Los datos de configuración de GFI EventsManager 2012 no se eliminan. Se copian en la nueva carpeta de instalación (*%icarpeta nstall%*\Data_Old). Los datos en esta carpeta se utilizan para conservar las configuraciones anteriores.

Nota

Pruebe la instalación para asegurarse de que que todos los componentes se hayan instalado correctamente. Para obtener más información, consulte Probar la instalación.

2.4 Instalar una nueva instancia de GFI EventsManager

Los componentes incluidos en la siguiente tabla se pueden instalar usando **EventsManager.exe**:

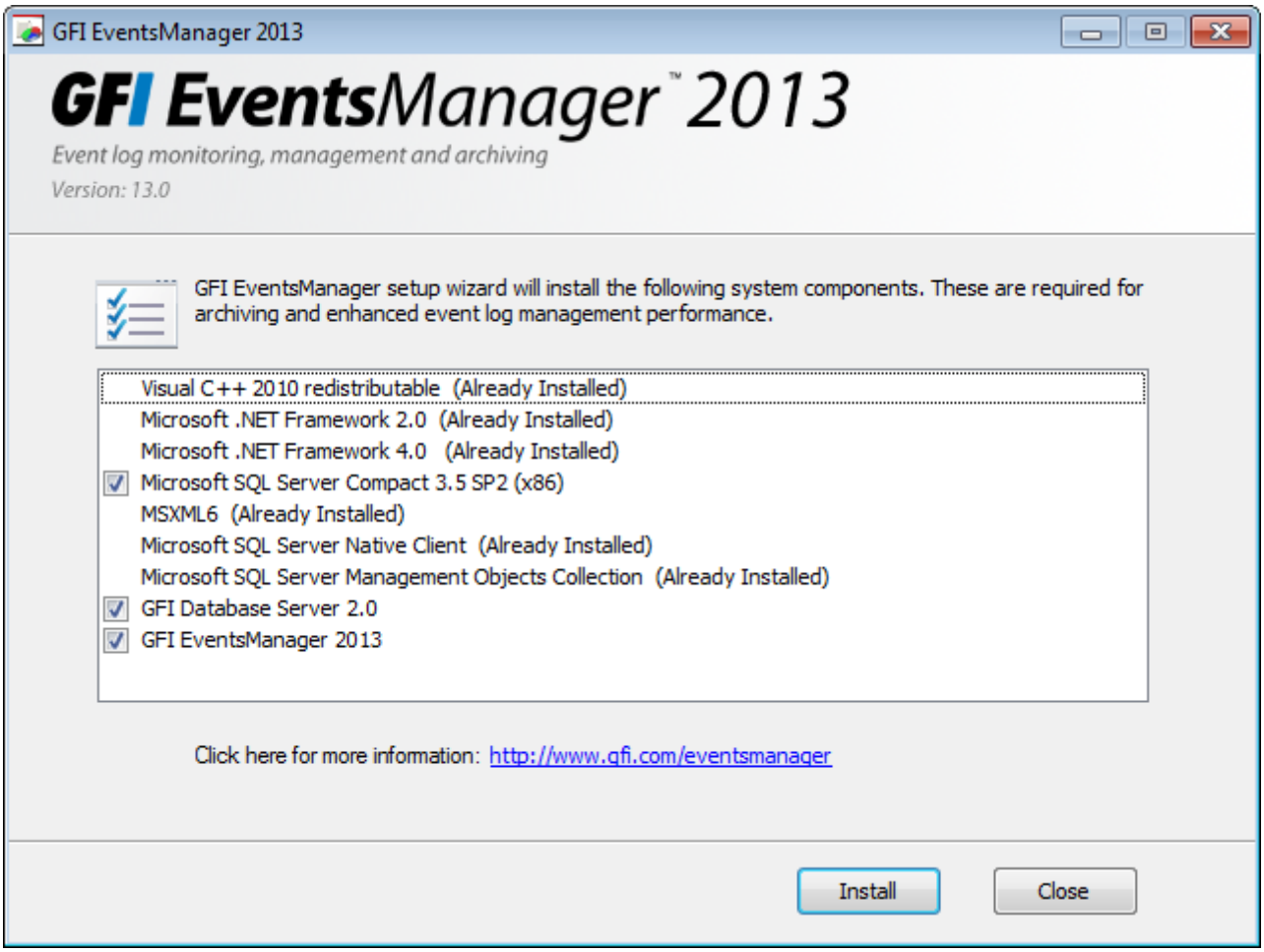
Tabla 11: Componentes instalados mediante EventsManager.exe

Componente	Descripción
Componentes del sistema	GFI EventsManager requiere los siguientes componentes del sistema para su funcionalidad completa: » Visual C++ 2010 redistribuible » Microsoft® .NET Framework 2.0 » Microsoft® .NET Framework 4.0 » Microsoft®SQL Server® Compact 3.5 SP2 » MSXML6 » Microsoft®SQL Server® Native Client » Microsoft® SQL Server® Management Objects Collection.
Servidor de bases de datos DLib	El servidor de bases de datos DLib es el componente donde GFI EventsManager almacena los registros procesados. El servidor de bases de datos se puede instalar en el mismo equipo que está ejecutando GFI EventsManager, así como en un equipo remoto independiente o unidad de red.
GFI EventsManager	El producto real desde donde se pueden administrar y supervisar los eventos generados por equipos y dispositivos en su red.

2.4.1 Procedimiento de instalación

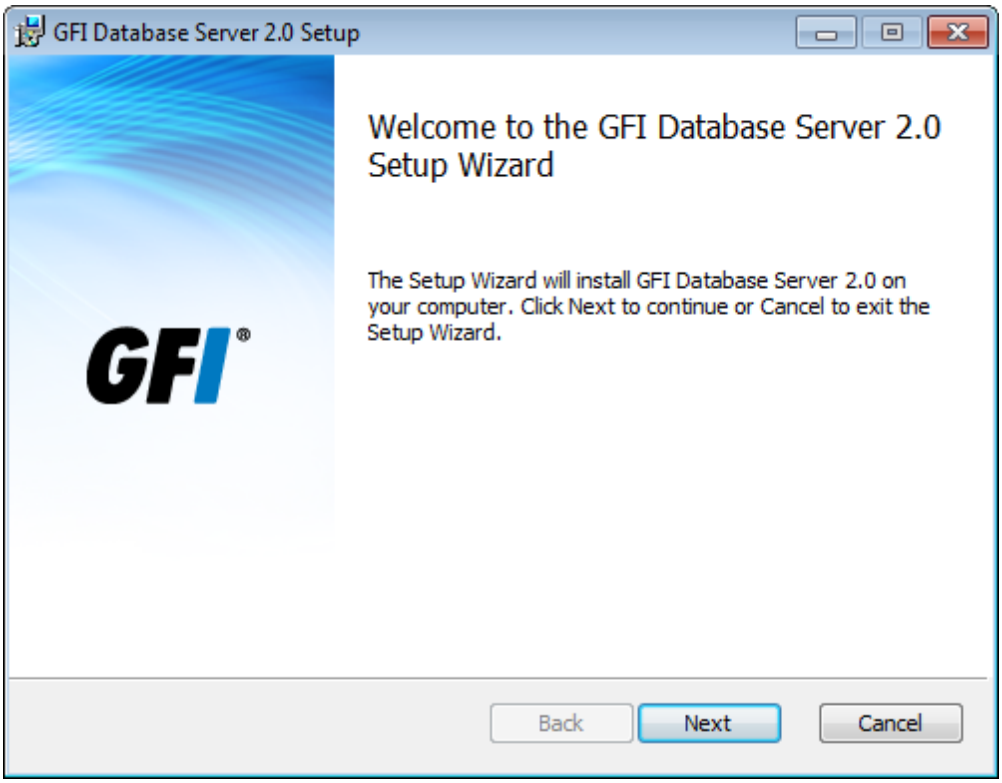
Para instalar GFI EventsManager:

1. Haga doble clic en **EventsManager.exe**.


GFI EventsManager 2013
GFI EventsManager 2013
Event log monitoring, management and archiving
Version: 13.0
GFI EventsManager setup wizard will install the following system components. These are required for archiving and enhanced event log management performance.
Visual C++ 2010 redistributable (Already Installed)
Microsoft .NET Framework 2.0 (Already Installed)
Microsoft .NET Framework 4.0 (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x86)
MSXML6 (Already Installed)
Microsoft SQL Server Native Client (Already Installed)
Microsoft SQL Server Management Objects Collection (Already Installed)
GFI Database Server 2.0
GFI EventsManager 2013
Click here for more information: http://www.gfi.com/eventsmanager
Install
Close

Captura de pantalla 18: Comprobación de requisitos previos a la actualización

2. El programa de instalación muestra una lista de componentes del sistema que deben instalarse antes de instalar el producto. Haga clic en **Install** para iniciar la instalación de los componentes del sistema que faltan (si es necesario).


GFI Database Server 2.0 Setup
Welcome to the GFI Database Server 2.0 Setup Wizard
The Setup Wizard will install GFI Database Server 2.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

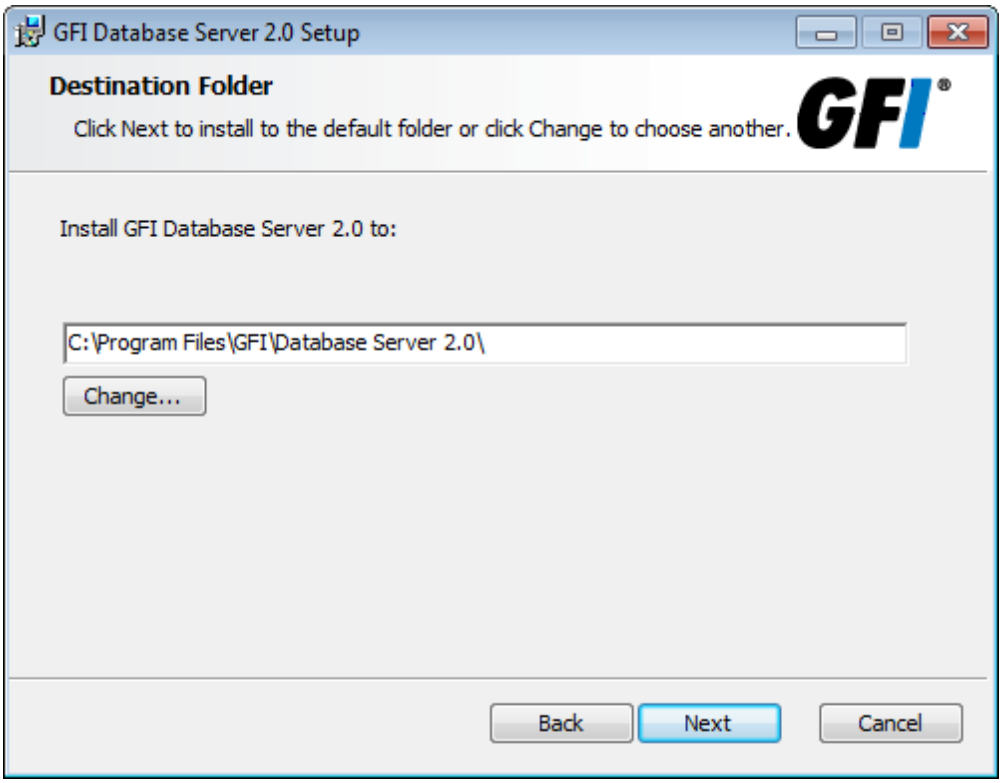
Captura de pantalla 19: Servidor de base de datos DLib

3. El asistente de instalación del servidor de base de datos DLib se abre automáticamente después de instalar los componentes del sistema. Haga clic en **Next** en la pantalla de bienvenida del asistente.

GFI Database Server 2.0 Setup
End-User License Agreement
Please read the following license agreement carefully
GFI
GFI® End-User License Agreement
For: GFI FaxMaker®; GFI MailArchiver®, GFI MailEssentials® and GFI MailSecurity®; GFI WebMonitor®; GFI LanGuard®;
GFI Network Server Monitor®; GFI EventsManager®; GFI BackUp®; GFI Device Warden™ and GFI EndPointSecurity®
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

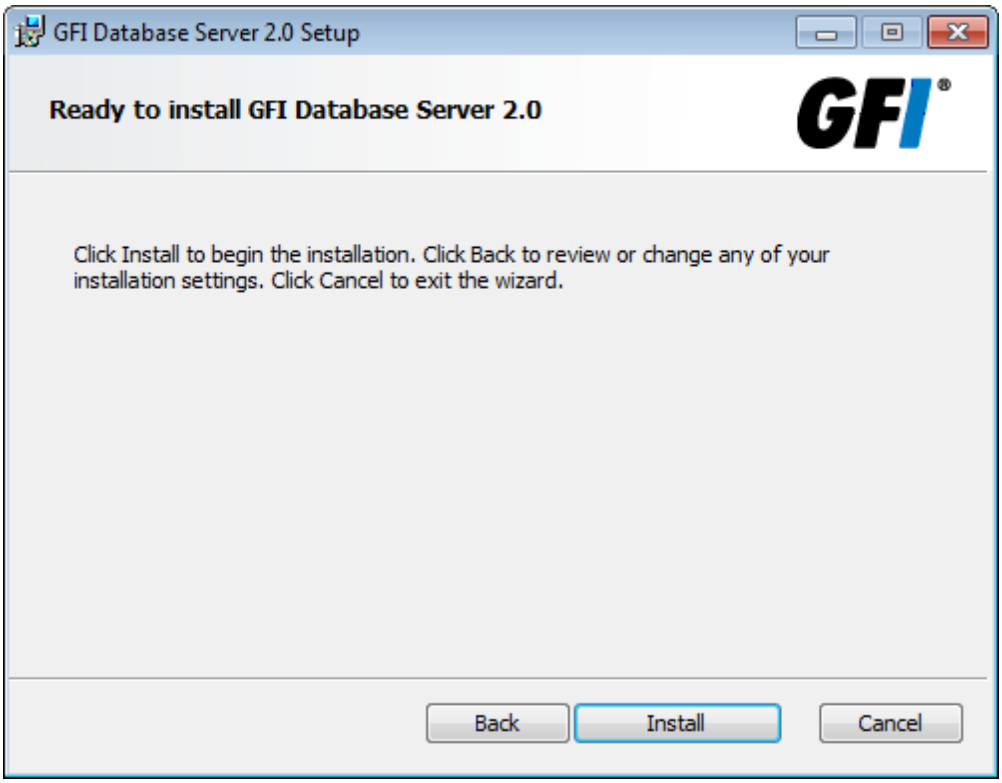
Captura de pantalla 20: EULA del servidor de base de datos DLib

4. Lea detenidamente el acuerdo de licencia. Seleccione **I accept the terms in the License Agreement** y haga clic en **Next**.



Captura de pantalla 21: Carpeta de instalación de DLib

5. Haga clic en **Next** para instalar el servidor de bases de datos en la carpeta predeterminada o haga clic en **Change...** para seleccionar una carpeta alternativa para la instalación.

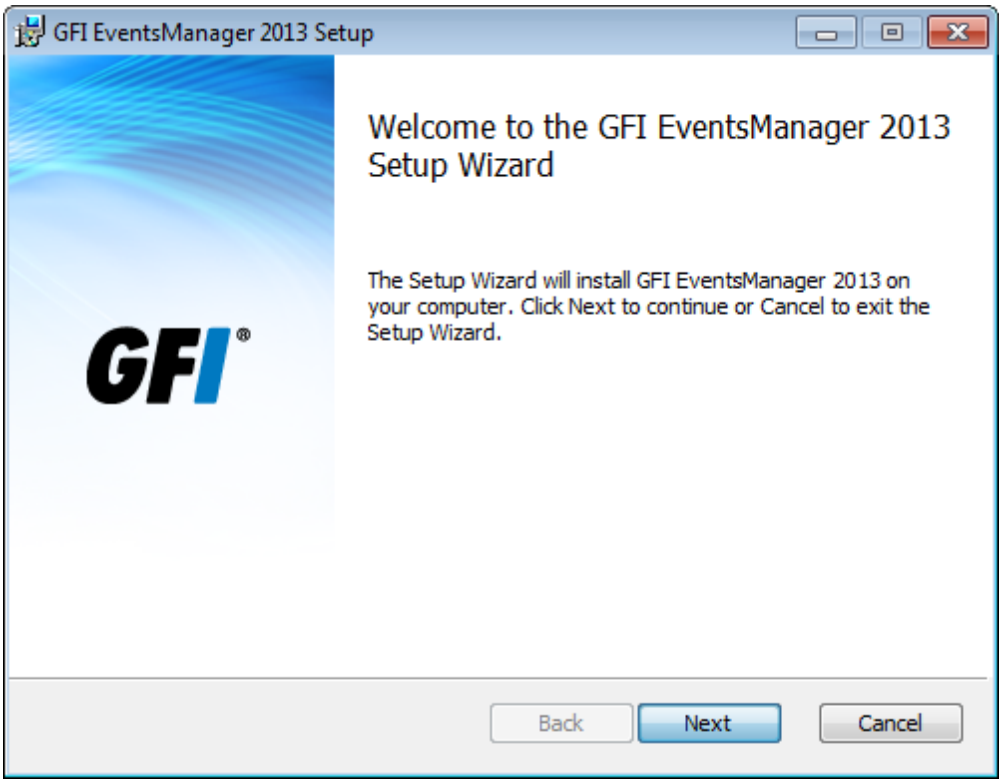

GFI Database Server 2.0 Setup
Ready to install GFI Database Server 2.0
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Captura de pantalla 22: Iniciar instalación del servidor de base de datos DLib

6. Haga clic en **Install** para iniciar la instalación del servidor de base de datos DLib. Haga clic en **Finish** cuando se le solicite.

Nota

Una vez instalado el servidor de bases de datos, el instalador abre automáticamente el asistente de instalación de la Consola de administración de GFI EventsManager.


GFI EventsManager 2013 Setup
Welcome to the GFI EventsManager 2013 Setup Wizard
The Setup Wizard will install GFI EventsManager 2013 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
GFI
Back
Next
Cancel

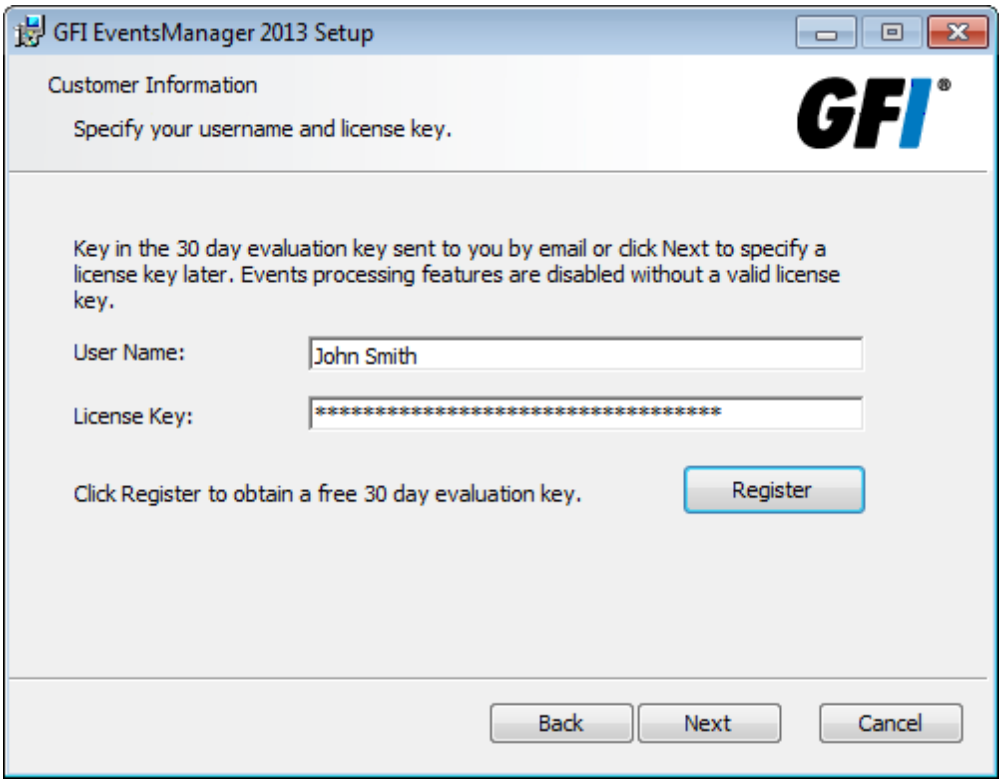
Captura de pantalla 23: Pantalla de bienvenida del asistente de instalación de GFI EventsManager

7. Haga clic en **Next** en la pantalla de bienvenida del asistente.

GFI EventsManager 2013 Setup
End-User License Agreement
Carefully read the following end user license agreement
GFI End-User License Agreement
For: GFI FaxMaker™; GFI MailArchiver™, GFI MailEssentials™ and GFI MailSecurity™; GFI WebMonitor™; GFI LanGuard™;
GFI Network Server Monitor™; GFI EventsManager™; GFI BackUp™; GFI Device Warden™ and GFI EndPointSecurity™
("Software")
I accept the terms in the License Agreement
Print
Back
Next
Cancel

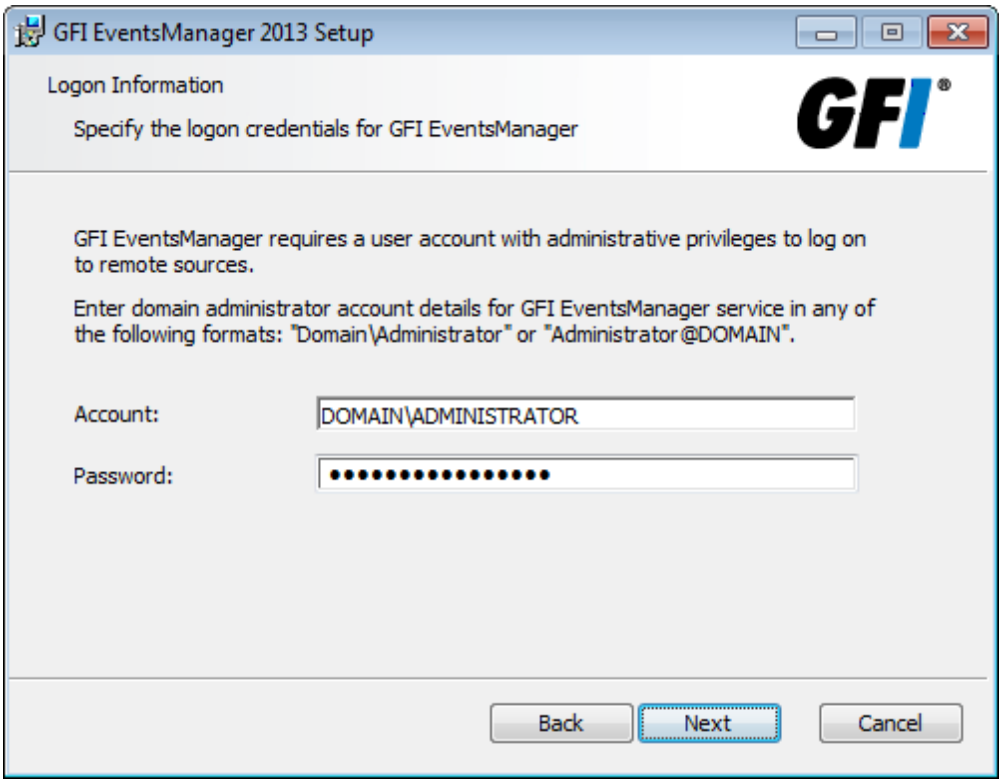
Captura de pantalla 24: EULA de GFI EventsManager

8. Lea detenidamente el acuerdo de licencia. Seleccione **I accept the terms in the License Agreement** y haga clic en **Next**.


GFI EventsManager 2013 Setup
Customer Information
Specify your username and license key.
Key in the 30 day evaluation key sent to you by email or click Next to specify a license key later. Events processing features are disabled without a valid license key.
User Name:
John Smith
License Key:
Click Register to obtain a free 30 day evaluation key.
Register
Back
Next
Cancel

Captura de pantalla 25: Detalles del registro de GFI EventsManager

9. Ingrese su nombre de usuario y la clave de licencia en los campos **User Name** y **License Key**. Para registrarse y acceder a una clave de licencia de evaluación gratuita de 30 días, haga clic en **Register**. Haga clic en **Siguiente**.

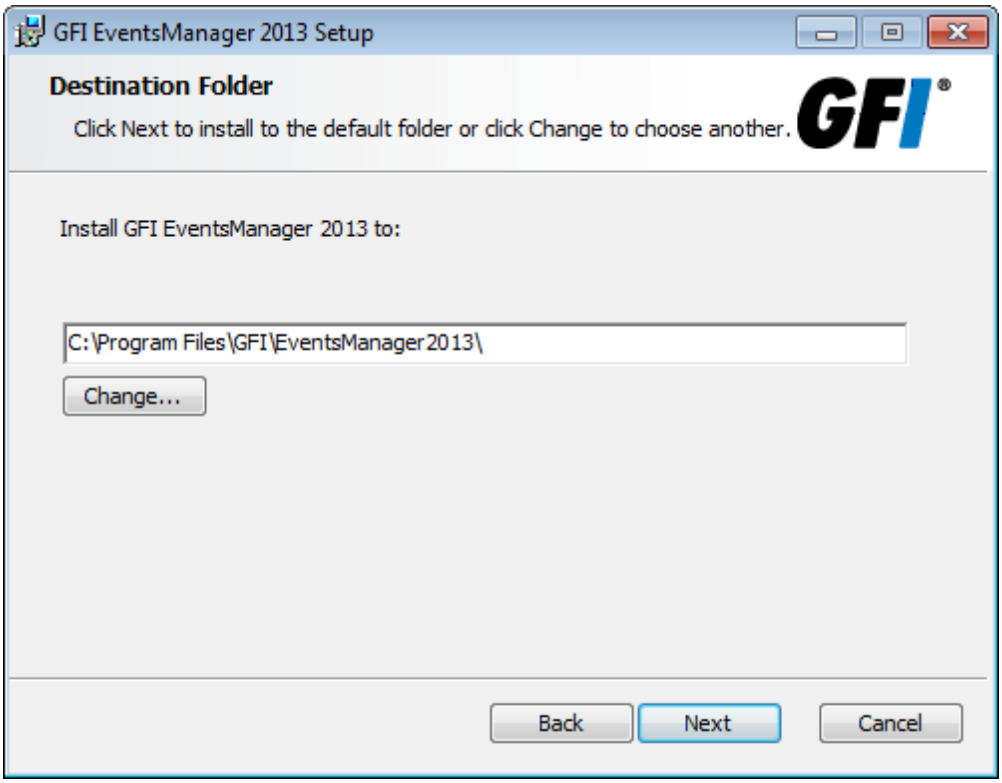

GFI EventsManager 2013 Setup
Logon Information
Specify the logon credentials for GFI EventsManager
GFI EventsManager requires a user account with administrative privileges to log on to remote sources.
Enter domain administrator account details for GFI EventsManager service in any of the following formats: "Domain\Administrator" or "Administrator@DOMAIN".
Account:
DOMAIN\ADMINISTRATOR
Password:
Back
Next
Cancel

Captura de pantalla 26: Credenciales de inicio de sesión remoto para supervisión de registros de eventos

10. Ingrese las credenciales de inicio de sesión que utiliza GFI EventsManager para iniciar sesión en equipos remotos.

Nota

Se recomienda usar un administrador de dominios o una cuenta con derechos administrativos sobre todos los equipos remotos administrados por GFI EventsManager.



Captura de pantalla 27: Carpeta de instalación de GFI EventsManager

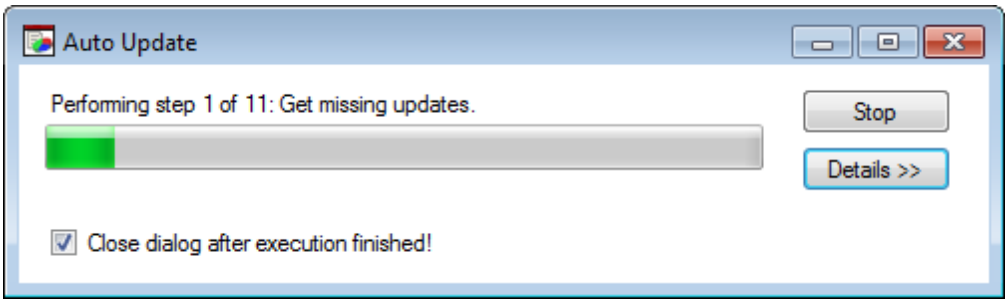
11. Haga clic en **Next** para instalar la Consola de administración en la carpeta predeterminada o haga clic en **Change...** para seleccionar una carpeta alternativa de instalación.

GFI EventsManager 2013 Setup
Ready to install GFI EventsManager 2013
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Captura de pantalla 28: Se completó la instalación de GFI EventsManager

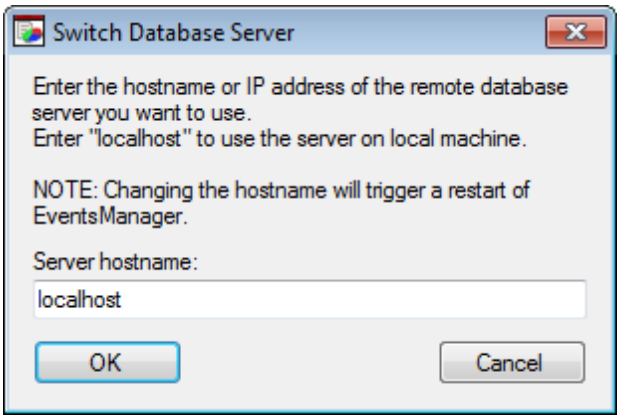
12. Haga clic en **Install** para iniciar la instalación.

13. Cuando la instalación se haya completado, haga clic en **Finish**.



Captura de pantalla 29: Comprobación automática de actualizaciones

14. Si GFI EventsManager detecta una conexión a Internet, automáticamente intenta descargar actualizaciones de productos de los servidores de actualización de GFI. Haga clic en **Details** para ampliar la sección de información del cuadro de diálogo Auto Update y ver las actualizaciones que se están descargando.


Switch Database Server
Enter the hostname or IP address of the remote database server you want to use.
Enter "localhost" to use the server on local machine.
NOTE: Changing the hostname will trigger a restart of EventsManager.
Server hostname:
localhost
OK
Cancel

Captura de pantalla 30: Definir el back-end de la base de datos

Nota

Después de aplicar las actualizaciones del producto, se abre el cuadro de diálogo **Switch Database Server**. Este cuadro de diálogo se utiliza para vincular la Consola de administración al servidor de bases de datos. Puede cambiar de servidor de bases de datos en la Consola de administración. Para obtener más información, consulte Cambiar de bases de datos de almacenamiento de archivos.

15. Especifique el equipo que tiene instalado el servidor de base de datos DLib. Si la base de datos que desea usar está en:

- Un equipo remoto: ingrese el **nombre de equipo** o la **dirección IP**
- El host local: ingrese el **localhost** (predeterminado).

Haga clic en **OK** para aceptar.

Nota

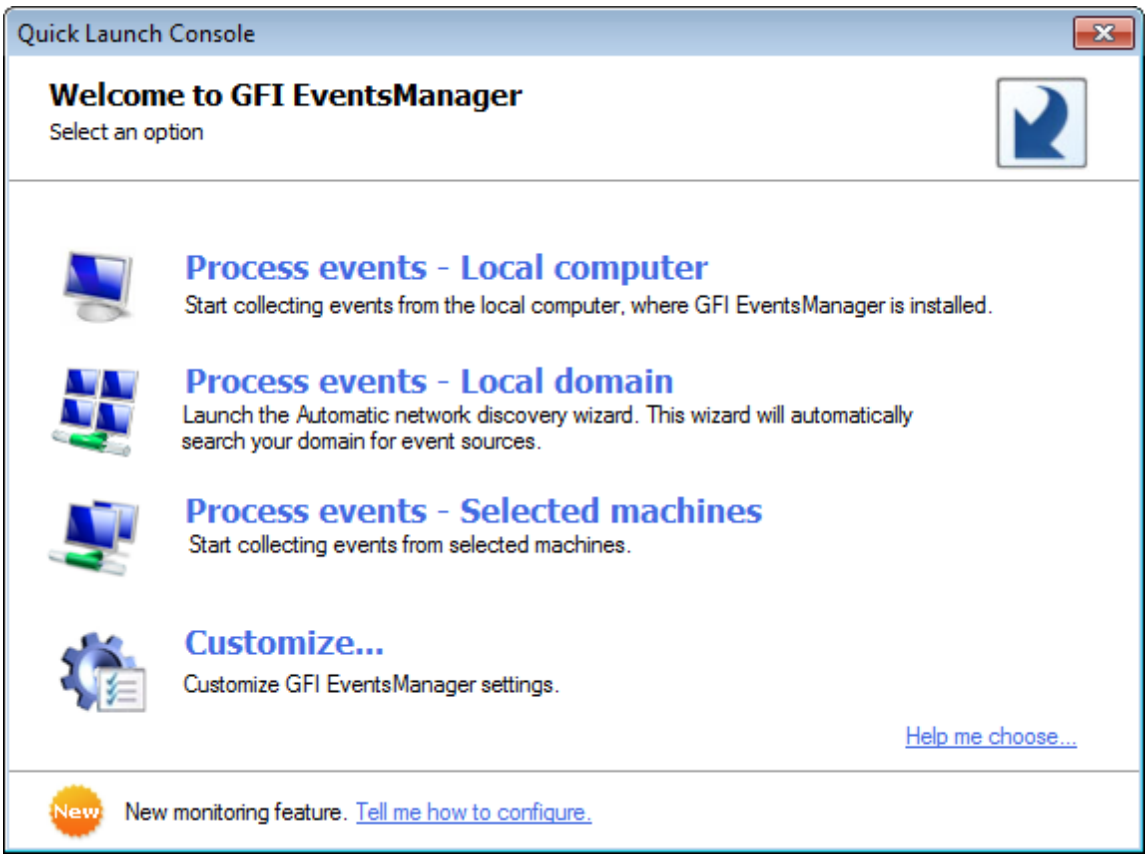
Una vez completada la instalación, la Consola de administración se abre automáticamente. Para ejecutarla manualmente, haga clic en **Inicio > Todos los programas > GFI EventsManager > Management Console**.

Nota

Pruebe la instalación para asegurarse de que que todos los componentes se hayan instalado correctamente. Para obtener más información, consulte Probar la instalación.

2.5 Probar la instalación

Una vez instalados todos los componentes necesarios, la Consola de administración se abre automáticamente. De forma predeterminada, está configurada para ejecutar la **Consola de inicio rápido** al iniciarse.


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Captura de pantalla 31: Ejecutar GFI EventsManager por primera vez

Seleccione una opción de la Consola de inicio rápido para procesar eventos o personalizar la configuración predeterminada:

Tabla 12: Opciones de la consola de inicio rápido

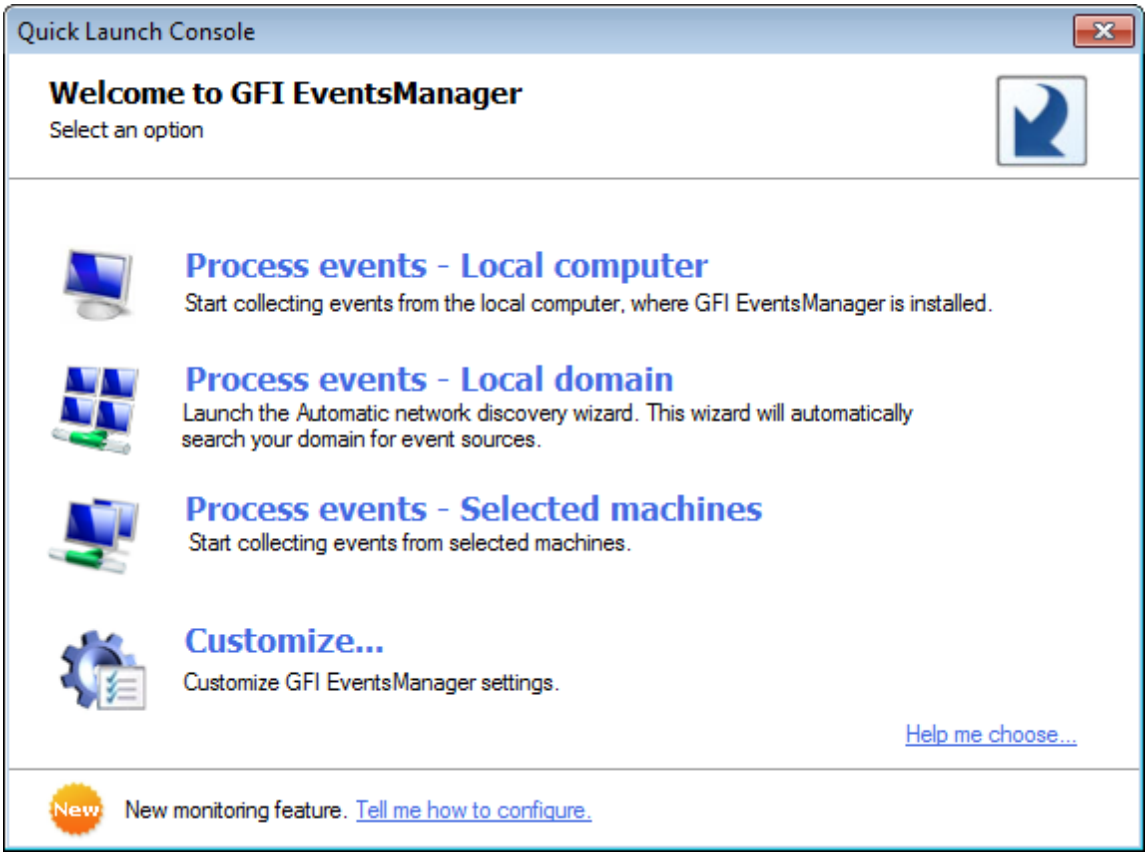
Opción	Descripción
Process events - Local computer	Se empiezan a procesar registros generados por el host de GFI EventsManager. **Nota** Para obtener más información, consulte Procesar eventos - Equipo local.
Process events - Local domain	Se empiezan a procesar registros generados por equipos y dispositivos de red en el mismo dominio que el host de GFI EventsManager. **Nota** Para obtener más información, consulte Procesar eventos - Dominio local.

Opción	Descripción
Process events - Selected machines	Se empiezan a procesar registros generados por uno o varios equipos específicos. **Nota** Para obtener más información, consulte Procesar eventos - Máquinas seleccionadas.
Customize...	Permite personalizar la configuración predeterminada, por ejemplo: » Orígenes de eventos y tipos de registro » Reglas de procesamiento de eventos » Operaciones de base de datos » Destinatarios de las alertas » Opciones de alerta » Supervisión activa.

2.5.1 Eventos del proceso - Equipo local

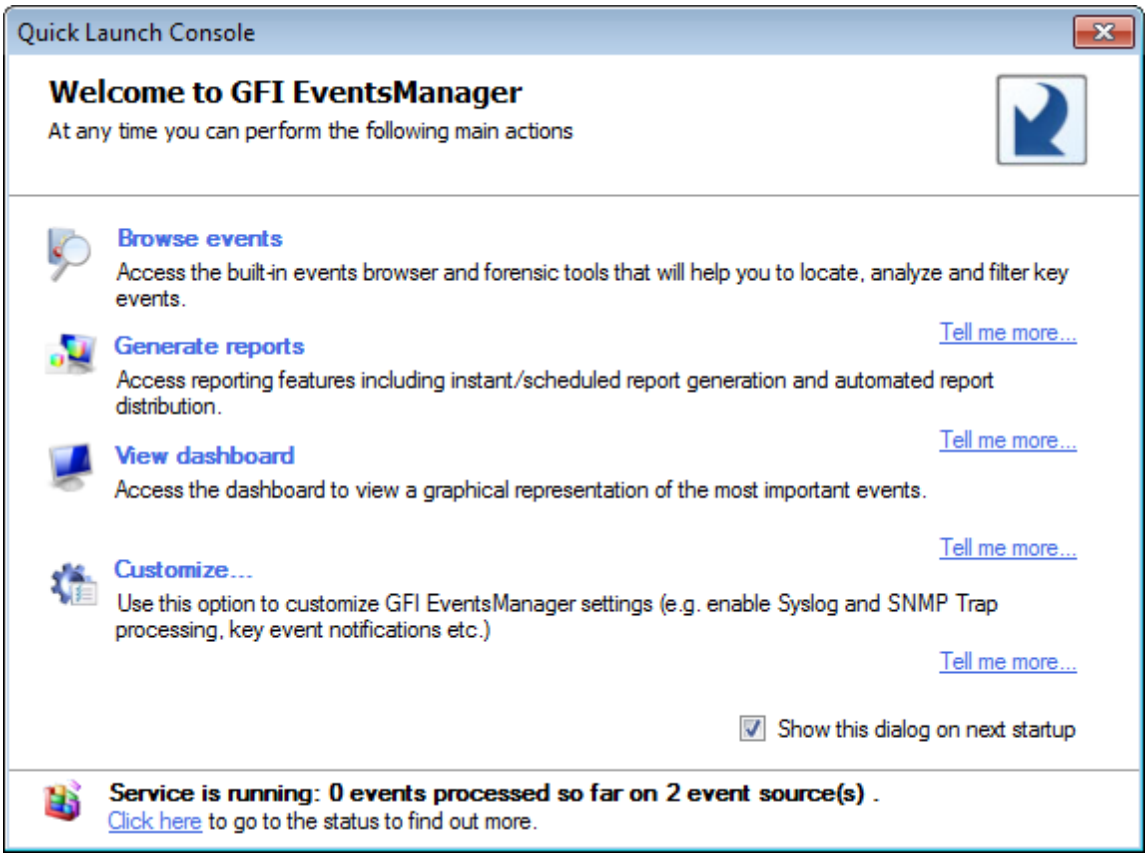
Esta opción le permite agregar automáticamente el host local como orígenes de eventos e iniciar el procesamiento de registros generados por este.

Para procesar eventos del equipo local:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Captura de pantalla 32: Eventos del proceso - Equipo local

1. Haga clic en **Process events - Local computer**.


Quick Launch Console
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyze and filter key events.
Tell me more...
Generate reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more...
View dashboard
Access the dashboard to view a graphical representation of the most important events.
Tell me more...
Customize...
Use this option to customize GFI EventsManager settings (e.g. enable Syslog and SNMP Trap processing, key event notifications etc.)
Tell me more...
Show this dialog on next startup
Service is running: 0 events processed so far on 2 event source(s) .
Click here to go to the status to find out more.

Captura de pantalla 33: Acciones principales de la consola

2. Después de que los registros del host local comiencen a procesarse, usted puede:

Tabla 13: Opciones de la consola de inicio rápido

Ícono	Descripción
	Buscar eventos Permite acceder a las herramientas forenses y de eventos incorporadas que lo ayudan a localizar, analizar y filtrar los eventos clave. Para obtener más información, consulte Buscar eventos almacenados.
	Generar informes Permite acceder a las características de informes, incluso la generación de informes instantáneos/programados y la distribución automatizada de informes. Para obtener más información, consulte Informes.
	Ver panel Permite acceder al panel de estado de GFI EventsManager. Esto le permite ver representaciones gráficas de los eventos más importantes recopilados y procesados por GFI EventsManager. Para obtener más información, consulte Supervisión de actividad.
	Personalizar Permite personalizar la configuración de GFI EventsManager, incluso habilitar Syslog, el procesamiento de captura SNMP, las comprobaciones del sistema, las notificaciones de eventos clave y más. Para obtener más información, consulte: » Administrar orígenes de eventos » Configurar reglas de procesamiento de eventos » Configurar opciones de mantenimiento de la base de datos » Configurar alertas y acciones predeterminadas » Configurar la supervisión activa

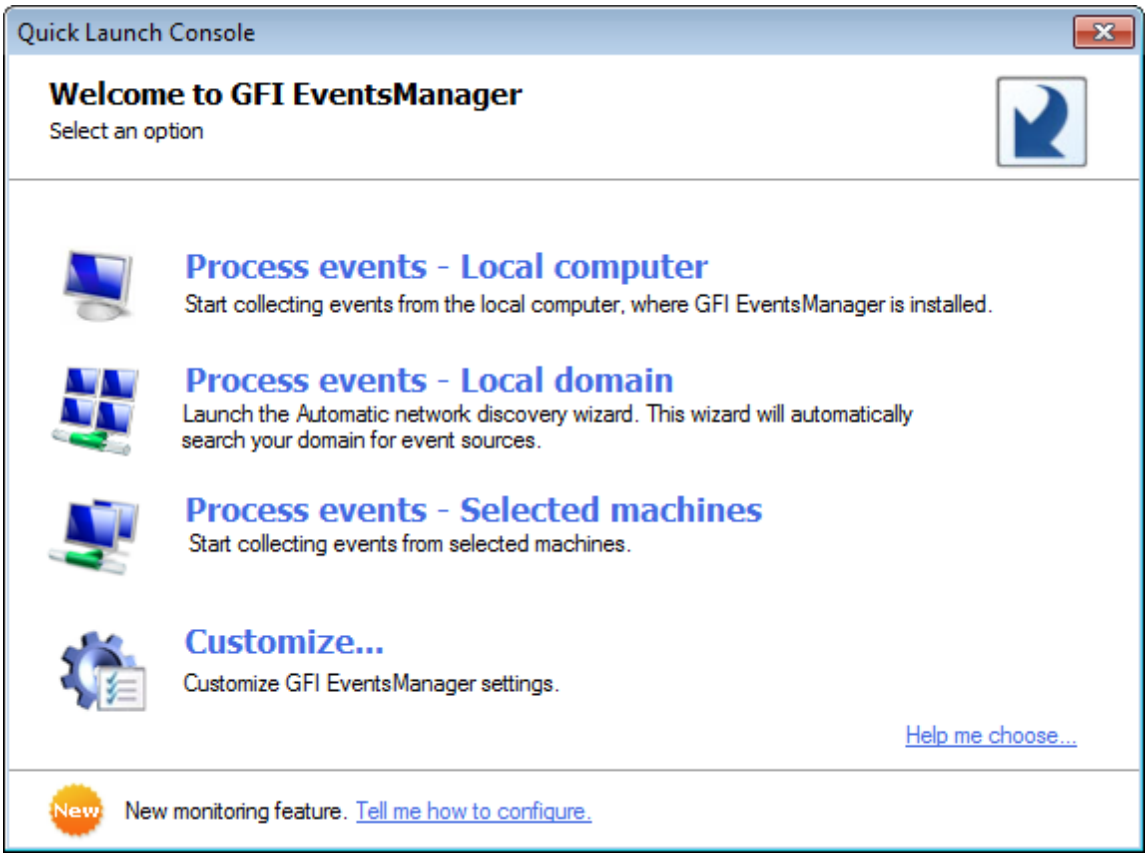
Nota

Para verificar que los registros se procesen correctamente, vaya a la ficha **Status > Job Activity** y compruebe que haya registros de actividad en la sección **Operational History**.

2.5.2 Eventos del proceso - Dominio local

Esta opción le permite agregar uno o más equipos que estén en el mismo dominio o grupo de trabajo que GFI EventsManager. El asistente de detección automática de red le permite seleccionar el tipo de orígenes de eventos que desea agregar y, a continuación, presenta una lista de los orígenes que se detecten.

Para procesar los eventos desde los equipos en el mismo dominio/grupo de trabajo:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Captura de pantalla 34: Eventos del proceso - Dominio local

1. Haga clic en **Process events - Local domain**. Se abre el asistente **Automatic Network Discovery**.

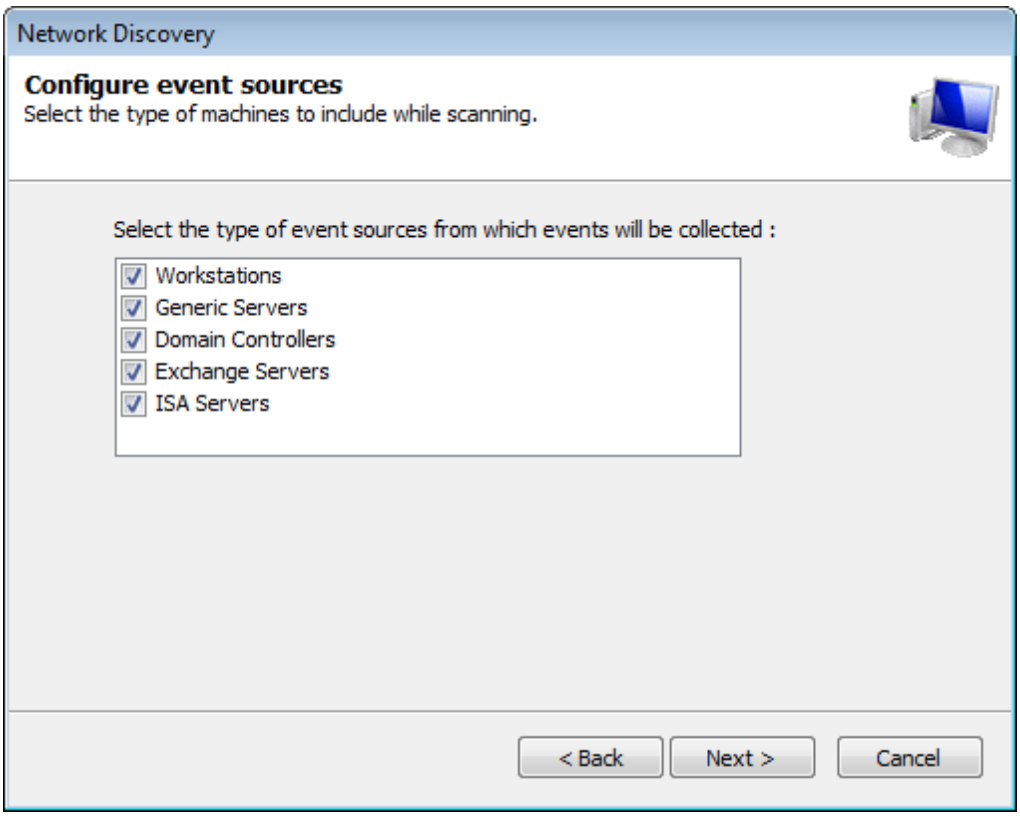
Nota

El asistente también se puede iniciar desde la ficha **Configuration> Event Sources**. En el panel izquierdo, haga clic con el botón secundario en **All event sources** y seleccione **Scan local domain**.

Network Discovery
Welcome to the Automatic network discovery wizard
This wizard searches the entire network for computers and servers.
Stage 1: Configure the event sources to include when scanning the local domain.
Stage 2: Search network for target computers. The wizard will collect information from all network computers using credentials used by the EventsManager Service.
Stage 3: Select network computers. Selected computers will be added as event sources.
Finish
< Back
Next >
Cancel

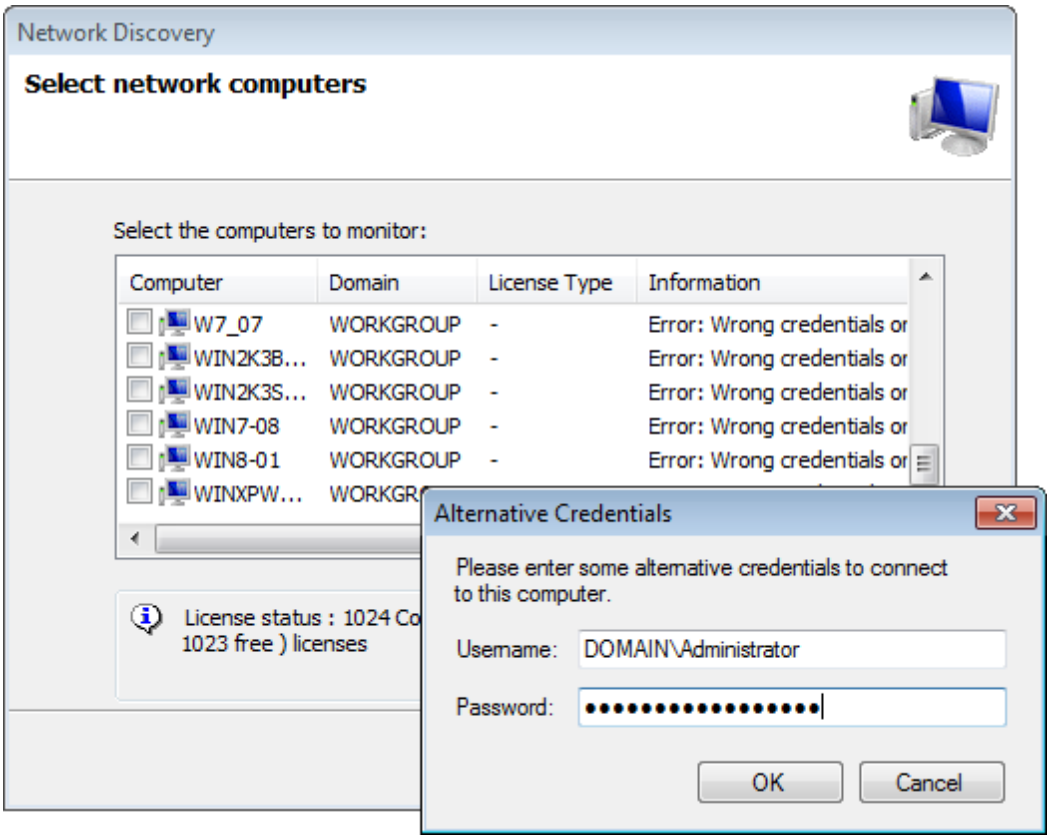
Captura de pantalla 35: Asistente de detección automática

2. Haga clic en **Next** en la pantalla de bienvenida del asistente.



Captura de pantalla 36: Seleccionar los tipos de orígenes de eventos que desea detectar en la red

3. Seleccione el tipo de orígenes de eventos que el asistente intentará detectar en la red. Haga clic en **Siguiente**.



Captura de pantalla 37: Buscar el progreso de red

Nota

Si GFI EventsManager detecta equipos que no se pueden registrar usando las credenciales proporcionadas, la aplicación le permite especificar credenciales de inicio de sesión alternativas para cada equipo que seleccione.

4. Seleccione un equipo de la lista e ingrese el nombre de usuario y la contraseña. Haga clic en **OK** para cerrar el cuadro de diálogo **Alternative Credentials**.

Nota

Repita este paso hasta que haya agregado todos los orígenes necesarios.

5. Haga clic en **Next** y en **Finish**.

Nota

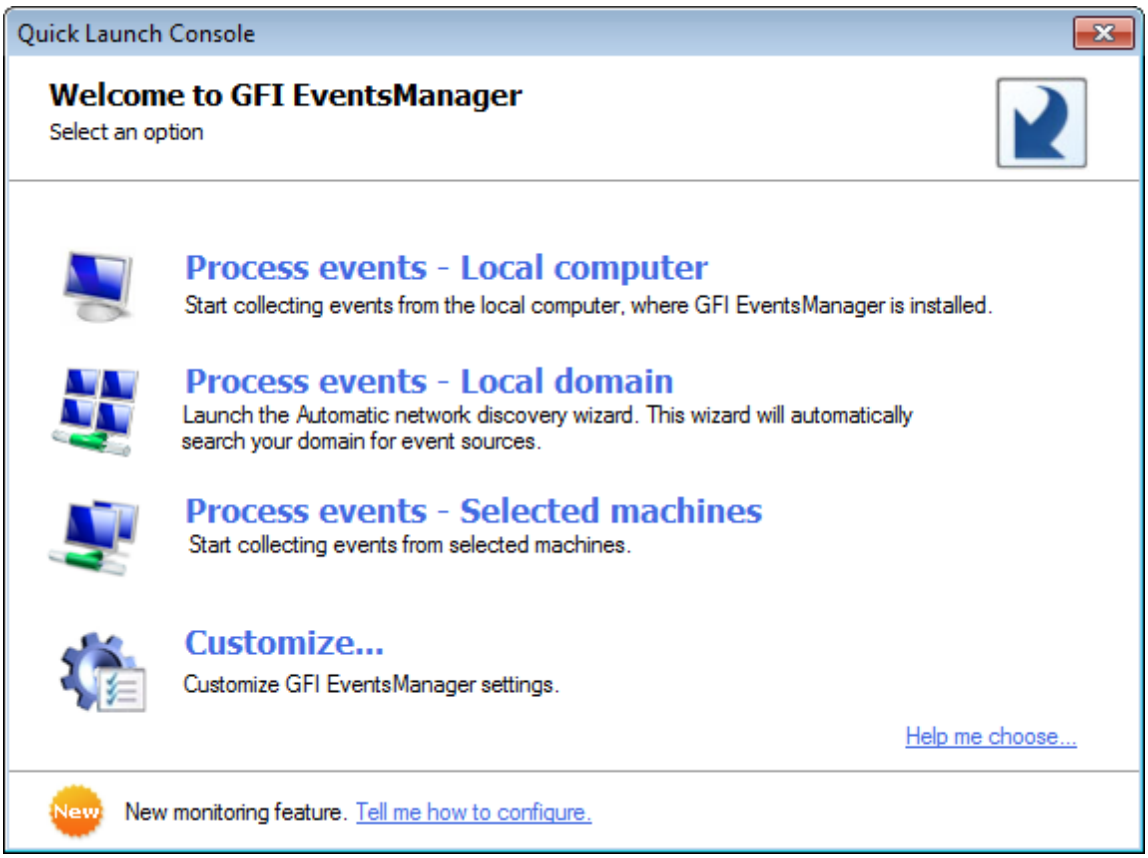
Para agregar automáticamente nuevos equipos que están vinculados al mismo dominio/grupo de trabajo que GFI EventsManager, debe configurar las opciones de sincronización. Para obtener más información, consulte Agregar orígenes de eventos automáticamente.

2.5.3 Eventos de proceso - Máquinas seleccionadas

Esta opción le permite agregar equipos específicos de forma manual al:

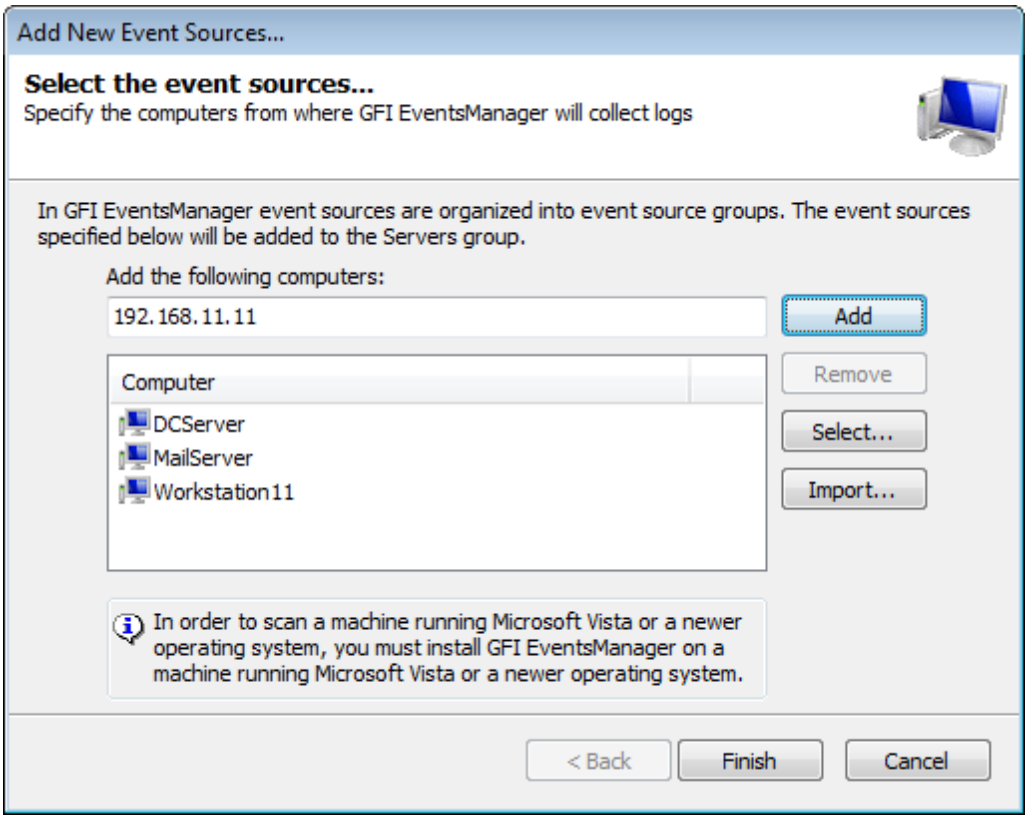
- Ingresar nombres de equipos y direcciones IP
- Seleccionar equipos desde dominios y grupos de trabajo accesibles
- Importar equipos desde un archivo de texto que contiene un único nombre de equipo por línea

Para procesar los eventos de las máquinas seleccionadas:


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...
New
New monitoring feature. Tell me how to configure.

Captura de pantalla 38: Eventos de proceso - Máquinas seleccionadas

1. Haga clic en **Process events - Selected machines.**
2. Se abre el cuadro de diálogo **Add New Event Source .**


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Servers group.
Add the following computers:
192.168.11.11
Add
Computer
DCServer
MailServer
Workstation11
Remove
Select...
Import...
In order to scan a machine running Microsoft Vista or a newer operating system, you must install GFI EventsManager on a machine running Microsoft Vista or a newer operating system.
< Back
Finish
Cancel

Captura de pantalla 39: Agregar nuevo asistente de origen de eventos

3. En la siguiente tabla, se describen las opciones disponibles:

Tabla 14: Agregar nuevos orígenes de eventos manualmente

Opción	Descripción
Add	Ingrese el nombre del equipo o la dirección IP en el campo **Add the following computers**. Haga clic en **Add** para agregar el equipo especificado en la lista **Computer**. **Nota** Repita este paso hasta que haya agregado todos los orígenes de eventos al grupo seleccionado. **Nota** Puesto que los syslog y las capturas SNMP utilizan direcciones IP para determinar el origen de un evento, se recomienda utilizar la dirección IP de origen en lugar del nombre del equipo al agregar orígenes de syslog y capturas SNMP.
Remove	Seleccione uno o varios equipos de la lista **Computer** y haga clic en **Remove** para eliminarlos de la lista.
Select...	Haga clic en **Select...** para abrir el cuadro de diálogo **Select Computers...**: 1. En el menú desplegable **Domain**, seleccione el dominio en el que desea buscar orígenes disponibles y haga clic en **Search**. 2. En la lista de resultados de búsqueda, seleccione los equipos que desee agregar. 3. Haga clic en **OK** para cerrar el cuadro de diálogo **Select Computers...** y volver al cuadro de diálogo **Add New Event Sources...**.
Import...	Haga clic en **Import...** para importar equipos desde un archivo de texto. Asegúrese de que el archivo de texto contenga solamente un nombre de equipo o dirección IP por línea.

4. Haga clic en **Finish** para finalizar la configuración. GFI EventsManager intenta analizar automáticamente los orígenes de eventos agregados con las credenciales de inicio de sesión predefinidas. Para obtener más información, consulte Configurar credenciales de inicio de sesión de orígenes de eventos.

Nota

Si la sincronización no está activada, puede usar **Network Discovery Wizard** para buscar y agregar orígenes de eventos de forma automática. Para iniciar el asistente **Network Discovery Wizard**, haga clic con el botón secundario en **All event sources** en el árbol de orígenes de eventos y seleccione **Scan local domain**. Para obtener más información, consulte Agregar orígenes de eventos automáticamente

Nota

Para verificar que los registros se procesen correctamente, vaya a la ficha **Status** > **Job Activity** y compruebe que haya registros de actividad en la sección **Operational History**.

3 Obtención de resultados

En este capítulo, se brinda información acerca de cómo usar GFI EventsManager para lograr resultados. La información provista lo ayuda a llevar a cabo investigaciones forenses positivas y supervisiones del sistema. También le permite alcanzar resultados positivos de cumplimiento legal, al tiempo que garantiza la seguridad de la red en todo momento.

Temas de este capítulo:

3.1 Lograr la seguridad de la red 63

3.2 Supervisar eficientemente el estado del sistema 65

3.3 Lograr el cumplimiento con PCI DSS 67

3.1 Lograr la seguridad de la red

Muchas empresas consideran erróneamente que el acceso no autorizado es simplemente una amenaza externa. La mayoría de las amenazas a la seguridad corporativa en realidad provienen de fuentes internas, contra las que un servidor de seguridad no ofrece ninguna protección. Una buena estrategia de seguridad incluye la supervisión en tiempo real de los eventos de seguridad críticos y el análisis periódico de los registros de seguridad de sus sistemas para que pueda detectar y responder rápidamente a los ataques.

La seguridad de la red se define como un conjunto de normas y políticas que adopta el administrador de red para supervisar y prevenir el mal uso y el acceso no autorizado a una red. Para definir una estrategia de red segura y eficaz, siga los pasos que se describen a continuación:

1. Agregue usuarios y grupos a la consola de administración

Varios usuarios pueden administrar GFI EventsManager. Puede vincular la actividad de la consola a los diferentes usuarios mediante la creación de un usuario para cada persona que tenga acceso a la consola e implemente cambios en las configuraciones.

- Cree usuarios para poder auditar la actividad individual. Para obtener más información, consulte Administrar cuentas de usuario.
- Cree grupos de usuarios para poder administrar varios usuarios a la vez. Para obtener más información, consulte Administrar grupos de usuarios.

2. Configure las opciones de seguridad de la consola

GFI EventsManager le permite configurar las opciones de seguridad de la consola para facilitar la protección de la información confidencial.

- Habilite el sistema de inicio de sesión de GFI EventsManager para que se pueda realizar un seguimiento individual de los usuarios. Para obtener más información, consulte Habilitar el sistema de inicio de sesión.
- Configure opciones de anonimización para que los usuarios no autorizados no tengan acceso a la información confidencial dentro de la consola de administración. Para obtener más información, consulte Anonimización.
- Habilite la auditoría de usuarios para que se pueda crear un registro de actividad de cada usuario que cambie las configuraciones del sistema. Para obtener más información, consulte Auditar la actividad de la consola.

3. Configure alertas y acciones predeterminadas

GFI EventsManager le permite realizar un seguimiento de la actividad de la red en tiempo real al activar alertas, ejecutar secuencias de comandos y llevar a cabo otras operaciones cuando se recopilan ciertos registros de eventos.

- Configure los destinatarios de alertas y la configuración de notificación por SMS, correo electrónico, redes y mensajes SNMP. Para obtener más información, consulte Configurar opciones de alerta.
- Configure las operaciones que se llevan a cabo cuando se detectan atributos específicos de un registro de eventos. Para obtener más información, consulte Configurar acciones de clasificación predeterminadas.

4. Agregue orígenes de eventos

Si todavía no lo hizo, agregue los orígenes de eventos que desea asegurar.

- Agregue los orígenes de eventos de forma manual al especificar las direcciones IP o los nombres de equipos. Para obtener más información, consulte Agregar orígenes de eventos manualmente.
- Agregue los orígenes de eventos de forma automática, no bien se unan al dominio o a la red. Para obtener más información, consulte Agregar orígenes de eventos automáticamente.

5. Habilite los permisos de auditoría de los orígenes de eventos

A fin de auditar los orígenes de eventos, se deben habilitar las opciones de auditoría en el sistema operativo de origen.

- Habilite las opciones de auditoría de forma manual para cada equipo. Para obtener más información, consulte Activar permisos de orígenes de eventos manualmente.
- Active las opciones de auditoría de forma automática para grupos más grandes de equipos. Para obtener más información, consulte Activar permisos de orígenes de eventos automáticamente.

6. Recopile los registros de eventos

Comience a recopilar los registros de eventos que generaron las fuentes agregadas en el paso anterior. Los registros de eventos se pueden recopilar no bien se agrega el origen. Sin embargo, puede personalizar incluso más la configuración de orígenes de eventos para recuperar información específica.

- Configure las propiedades de orígenes de eventos, como las credenciales de inicio de sesión, el tipo de licencia y otras opciones. Para obtener más información, consulte Configurar propiedades de orígenes de eventos.
- Configure los orígenes de eventos para recopilar y procesar los registros de eventos de Windows, los mensajes de captura SNMP, los registros de texto y mucho más. Para obtener más información, consulte Recopilar registros de eventos.

7. Analice los registros de eventos recopilados y supervise la actividad

Después de recopilar los registros de eventos requeridos, puede analizarlos en la aplicación Events Browser. Events Browser es el explorador de eventos que le permite crear reglas personalizadas a partir de los registros recopilados. Esto le permite activar alertas o acciones cuando se recopilan eventos del mismo tipo.

- Cree reglas basadas en eventos recopilados. Las reglas de procesamiento de eventos le permiten comprobar un registro de eventos y realizar acciones en función de los parámetros que se configuraron en el Paso 3. Para obtener más información, consulte Crear nuevas reglas a partir de eventos existentes.
- Supervise la actividad de administración de eventos de los paneles de información. Para obtener más información, consulte Supervisar actividades.

3.2 Supervisar eficientemente el estado del sistema

GFI EventsManager puede llevar a cabo comprobaciones exhaustivas del sistema en los servidores y las estaciones de trabajo. Aplica una supervisión activa para ayudarlo a detectar y resolver de manera proactiva los errores del sistema y los defectos del hardware a fin de evitar desastres en la red.

Las comprobaciones del sistema son capaces de supervisar los servidores críticos para la misión, incluso Microsoft®ISA Server®, Exchange Server®, SQL Server ® e IIS®. Incluso se les puede configurar para profundizar en los sistemas y supervisar las colas de correo electrónico, las puertas de enlace SMTP, la disponibilidad MAPI, los bloques defectuosos del disco duro, el espacio en disco y mucho más.

La supervisión de la eficacia de las reglas y las políticas aplicadas a los sistemas ayuda a determinar el grado de eficacia de los planes y las acciones en práctica.

---

1. Agregue orígenes de eventos

Una vez instalado, GFI EventsManager agrega automáticamente el host local a la lista de orígenes de eventos. Agregue otras fuentes de forma manual o automática, de acuerdo con sus preferencias.

- Agregue equipos manualmente especificando nombres de equipo, direcciones IP. Para obtener más información, consulte Agregar orígenes de eventos manualmente.
- Los equipos también se pueden agregar de forma automática no bien son detectados por GFI EventsManager. Para obtener más información, consulte Agregar orígenes de eventos automáticamente

---

2. Configure los orígenes de eventos

Configure las propiedades de orígenes de eventos para habilitar la supervisión activa y el procesamiento de eventos. Consulte las siguientes secciones para obtener información acerca de:

- Configurar propiedades de orígenes de eventos
- Configurar supervisión de orígenes de eventos
- Recopilar registros de eventos.

---

3. Configure alertas y acciones predeterminadas

Una de las características clave de GFI EventsManager es la capacidad de enviar notificaciones y realizar acciones predefinidas cuando se recopilan ciertos registros de eventos.

Planifique cómo se envían las notificaciones y configure el servidor de correo electrónico, la puerta de enlace SMS o la configuración de la red según corresponda. Agregue los destinatarios en GFI EventsManager a los que se envían las notificaciones.

Una vez completado este paso, configure las acciones predeterminadas que se deben llevar a cabo cuando se procesan eventos específicos. Consulte la siguiente sección para obtener información acerca de:

- Configurar la cuenta del administrador
- Administrar cuentas de usuario
- Configurar opciones de alerta
- Configurar acciones de clasificación predeterminadas

---

4. Configure la supervisión activa

Las comprobaciones de supervisión activa son parámetros condicionales que se ejecutan en los orígenes de eventos en base a una programación. Independientemente de si las condiciones de los parámetros se cumplen o no, las comprobaciones de supervisión generan registros de eventos.

El registro de eventos generado se puede combinar con las reglas de procesamiento de eventos para analizar más exhaustivamente el problema que generó el registro, enviar notificaciones, ejecutar secuencias de comandos e implementar medidas correctivas.

GFI EventsManager contiene algunas supervisiones activas genéricas que se pueden usar inmediatamente. También puede crear nuevas supervisiones y establecer la configuración granular para adquirir información precisa e importante. Consulte las siguientes secciones para obtener información acerca de:

- Supervisión activa
- Crear y configurar carpetas raíz
- Crear y configurar la supervisión activa
- Aplicar la supervisión activa
- Analizar la actividad de la supervisión activa

---

5. Configure las reglas de procesamiento de eventos

Las reglas de procesamiento de eventos son las comprobaciones condicionales que se ejecutan en los registros de eventos recopilados. Según la información que se encuentra en el registro de eventos (como **Log Type**, **Timestamp** y **Classification**), GFI EventsManager determina la acción que se debe realizar.

Cree nuevas reglas a partir de registros de eventos generados por los controles de supervisión activa para desencadenar operaciones automáticas correctivas cuando se detecta un error del sistema.

Opcionalmente, configure los orígenes de eventos para ejecutar reglas de estado del sistema en los registros de eventos recopilados. Consulte las siguientes secciones para obtener información acerca de:

- Reglas de procesamiento de eventos
- Acerca de las reglas de procesamiento de eventos
- Administrar carpetas de conjuntos de reglas
- Crear nuevas reglas a partir de eventos existentes
- Configurar condiciones de reglas
- Configurar orígenes de eventos para procesar registros con reglas de estado del sistema

---

6. Genere informes

GFI EventsManager le permite generar informes para el personal técnico de TI, así como informes de resumen ejecutivos para el personal de administración. Los informes lo ayudan a visualizar la información de red a través de gráficos y tablas, así como la información estadística que se proporciona en los informes.

GFI EndPointSecurity viene con una diversidad de informes predefinidos y también le permite crear nuevos informes o modificar los informes ya existentes.

- Informes disponibles
- Generar informes
- Administrar informes
- Crear informes personalizados
- Configurar condiciones de filtrado de informes

3.3 Lograr el cumplimiento con PCI DSS

El Estándar de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI) es una norma que define una lista de requisitos relacionados con la administración de la seguridad, las políticas, la arquitectura de la red y otras medidas que ayudan a proteger la cuenta de un cliente y los datos de las tarjetas de crédito.

El pleno cumplimiento con PCI DSS requiere una administración completa de los registros de eventos junto con informes exhaustivos; por lo tanto GFI EventsManager es una solución esencial para contribuir con su programa de cumplimiento de PCI. Para obtener más información acerca de cómo cumplir con PCI DSS, use los siguientes vínculos:

Documento sobre el cumplimiento de PCI DSS y productos de GFI Software

Consulte los documentos de GFI sobre el cumplimiento de PCI DSS:

- http://go.gfi.com/?pageid=EM_PCIDSS

¿Cómo GFI EventsManager puede contribuir al cumplimiento con PCI DSS?

- Supervisa regularmente las actividades de administración de eventos. Para obtener más información, consulte Supervisar actividades.
- Aplica reglas de procesamiento de eventos según la lista de requisitos de PCI DSS. Para obtener más información, consulte Reglas de procesamiento de eventos.
- Genera informes a intervalos regulares para supervisar los eventos. Para obtener más información, consulte Informes.

4 Administrar orígenes de eventos

Este capítulo proporciona información acerca de cómo agregar y administrar sus orígenes de eventos. Los orígenes de eventos son equipos y dispositivos conectados a la red a los que GFI EventsManager tiene acceso para procesarlos. La ficha secundaria Events Sources le permite organizar sus orígenes de eventos en grupos específicos. Puede crear nuevos grupos o utilizar los predeterminados para configurar y organizar distintivamente los orígenes de eventos.

Temas de este capítulo:

4.1 Agregar orígenes de eventos manualmente 69

4.2 Agregar orígenes de eventos automáticamente 70

4.3 Crear un nuevo grupo de orígenes de eventos 73

4.4 Configurar propiedades de orígenes de eventos 75

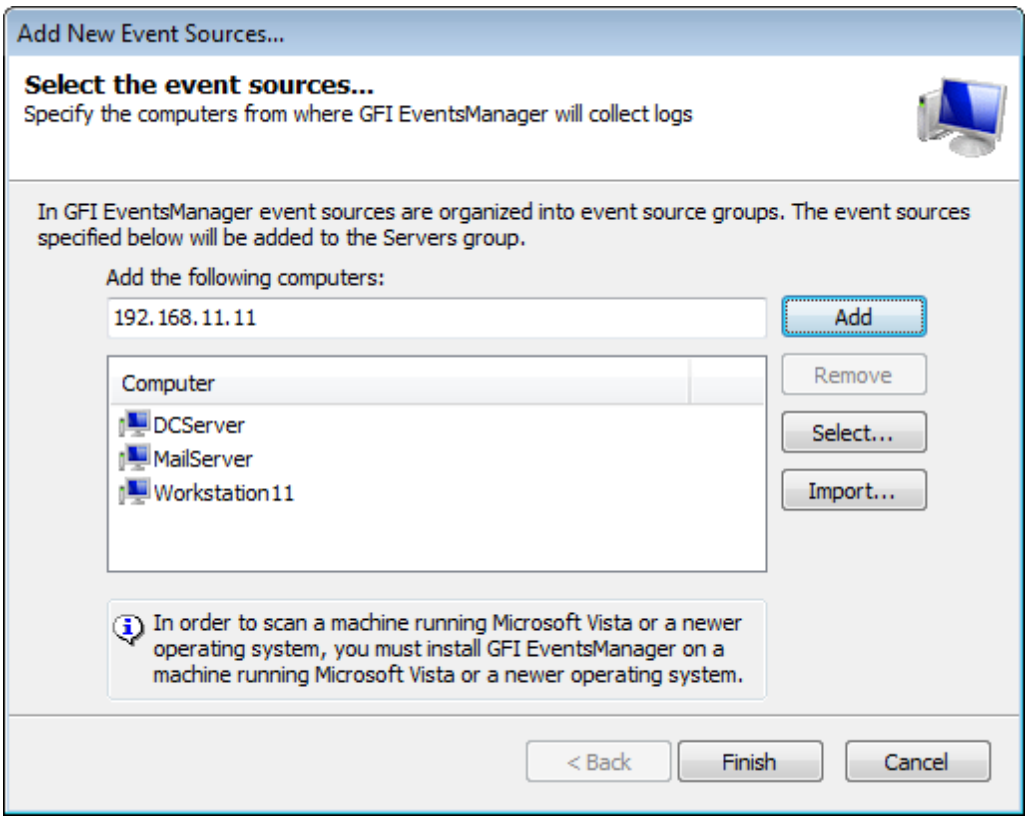
4.5 Orígenes de bases de datos 84

4.1 Agregar orígenes de eventos manualmente

Para agregar manualmente un nuevo origen de eventos a un grupo de equipos:

1. Haga clic en la ficha **Configuration > Event Sources** y en **Group Type**, seleccione **Event Sources Groups**.

2. Haga clic con el botón secundario en un grupo de equipos que desee y seleccione **Add new event source…**.


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Servers group.
Add the following computers:
192.168.11.11
Add
Remove
Select...
Import...
Computer
DCServer
MailServer
Workstation11
In order to scan a machine running Microsoft Vista or a newer operating system, you must install GFI EventsManager on a machine running Microsoft Vista or a newer operating system.
< Back
Finish
Cancel

Captura de pantalla 40: Agregar nuevo asistente de origen de eventos

3. En la siguiente tabla, se describen las opciones disponibles:

Tabla 15: Agregar nuevos orígenes de eventos manualmente

Opción	Descripción
Add	Ingrese el nombre del equipo o la dirección IP en el campo **Add the following computers**. Haga clic en **Add** para agregar el equipo especificado en la lista **Computer**. **Nota** Repita este paso hasta que haya agregado todos los orígenes de eventos al grupo seleccionado. **Nota** Puesto que los syslog y las capturas SNMP utilizan direcciones IP para determinar el origen de un evento, se recomienda utilizar la dirección IP de origen en lugar del nombre del equipo al agregar orígenes de syslog y capturas SNMP.
Remove	Seleccione uno o varios equipos de la lista **Computer** y haga clic en **Remove** para eliminarlos de la lista.
Select...	Haga clic en **Select...** para abrir el cuadro de diálogo **Select Computers...**: 1. En el menú desplegable **Domain**, seleccione el dominio en el que desea buscar orígenes disponibles y haga clic en **Search**. 2. En la lista de resultados de búsqueda, seleccione los equipos que desee agregar. 3. Haga clic en **OK** para cerrar el cuadro de diálogo **Select Computers...** y volver al cuadro de diálogo **Add New Event Sources...**.
Import...	Haga clic en **Import...** para importar equipos desde un archivo de texto. Asegúrese de que el archivo de texto contenga solamente un nombre de equipo o dirección IP por línea.

4. Haga clic en **Finish** para finalizar la configuración. GFI EventsManager intenta analizar automáticamente los orígenes de eventos agregados con las credenciales de inicio de sesión predefinidas. Para obtener más información, consulte Configurar credenciales de inicio de sesión de orígenes de eventos.

Nota

Si la sincronización no está activada, puede usar **Network Discovery Wizard** para buscar y agregar orígenes de eventos de forma automática. Para iniciar el asistente **Network Discovery Wizard**, haga clic con el botón secundario en **All event sources** en el árbol de orígenes de eventos y seleccione **Scan local domain**. Para obtener más información, consulte Agregar orígenes de eventos automáticamente

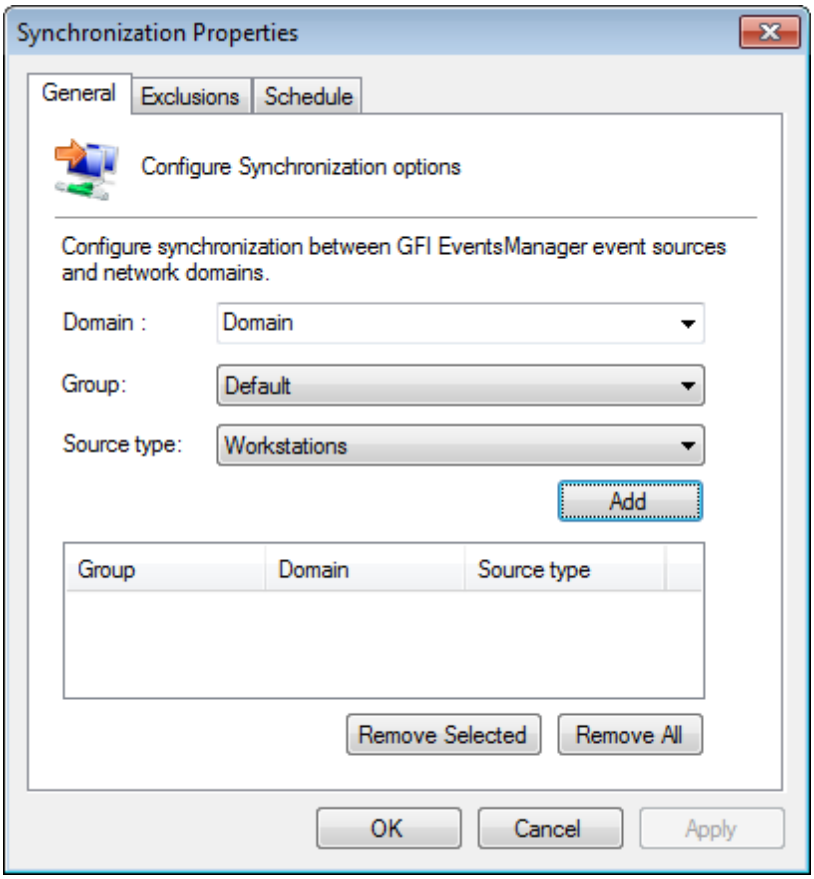
4.2 Agregar orígenes de eventos automáticamente

GFI EventsManager le permite sincronizar automáticamente los dominios con grupos de orígenes de eventos. Cuando se configura la sincronización, cada nuevo miembro del dominio se agrega automáticamente a la lista de orígenes de eventos de GFI EventsManager.

Para habilitar la sincronización automática:

1. Haga clic en la ficha **Configuration > Event Sources** y en **Group Type**, seleccione **Event Sources Groups**.

2. Haga clic en **All event sources** y seleccione **Edit synchronization options**.



Captura de pantalla 41: Ficha Synchronization properties - General

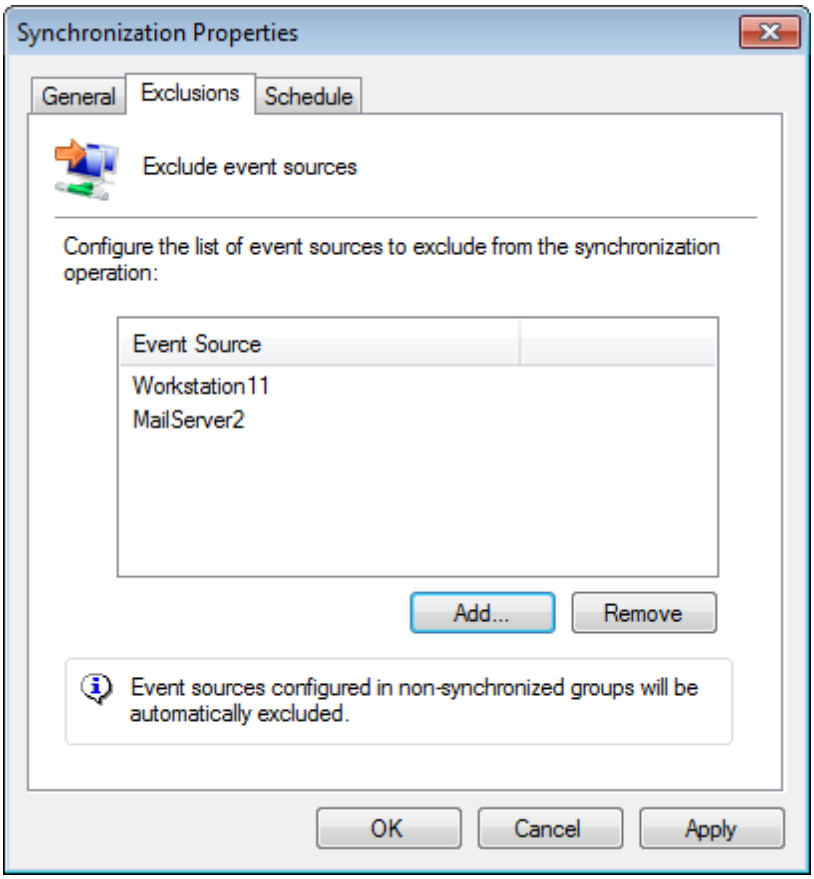
3. Seleccione la ficha **General** y configure las opciones que se describen a continuación:

Tabla 16: Ficha Synchronization properties - General

Opción	Descripción
Domain	Seleccione el nombre de dominio de la lista o ingrese un nombre de dominio válido.
Group	Seleccione el nombre del grupo de GFI EventsManager en el que desea agregar los orígenes de eventos detectados.
Source type	Seleccione el tipo de orígenes de eventos que GFI EventsManager buscará en el dominio especificado.

4. Para incluir la sincronización, haga clic en **Add**.

5. Repita los Pasos 3 a 4 para cada dominio que desee sincronizar.

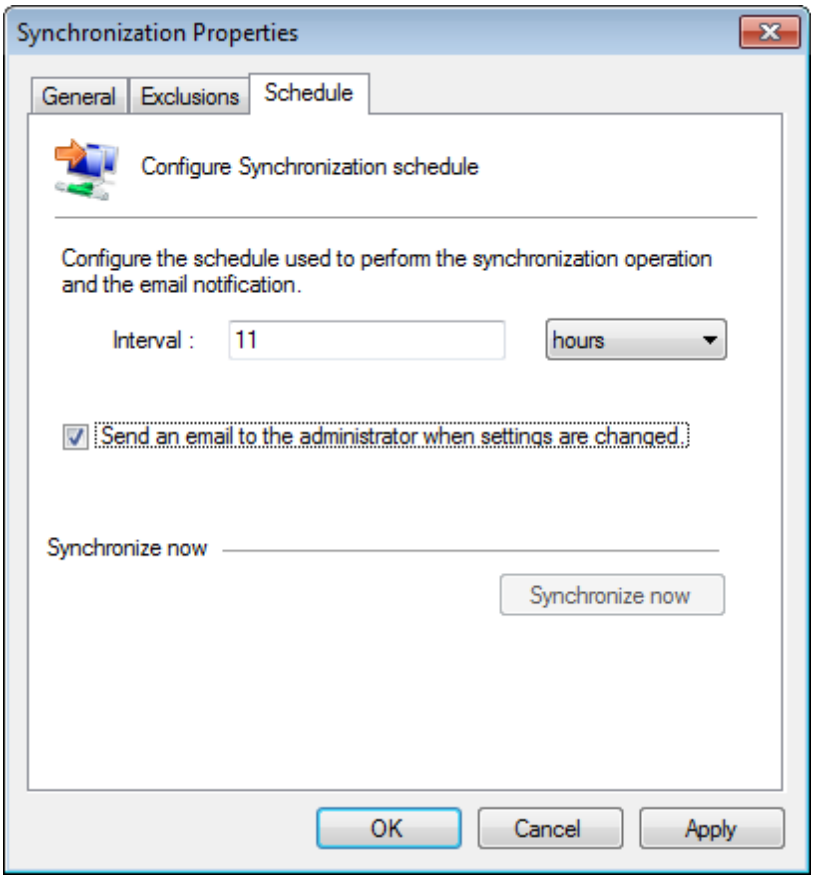


Captura de pantalla 42: Excluir equipos de la sincronización automática

6. (Opcional) Seleccione la ficha **Exclusions** para configurar la lista de equipos que serán excluidos de la sincronización. Haga clic en **Add** e ingrese el nombre del equipo que desea excluir.

> **Nota**
>
> Los orígenes de eventos que ya forman parte de un grupo de orígenes de eventos serán automáticamente excluidos de la sincronización.

7. Seleccione la ficha **Schedule** para configurar cuándo se debe realizar la sincronización.



Captura de pantalla 43: Ficha Synchronization properties -Schedule

8. Ingrese un intervalo válido en horas o días.

9. (Opcional) Seleccione **Send an email to the...** para enviar una notificación por correo electrónico cuando se cambian los orígenes de eventos después de la sincronización.

10. (Opcional) Haga clic en **Synchronize now** para sincronizar los orígenes de eventos inmediatamente.

11. Haga clic en **Apply** y **OK**.

Nota

No se pueden agregar orígenes de eventos manualmente a un grupo sincronizado en GFI EventsManager.

4.3 Crear un nuevo grupo de orígenes de eventos

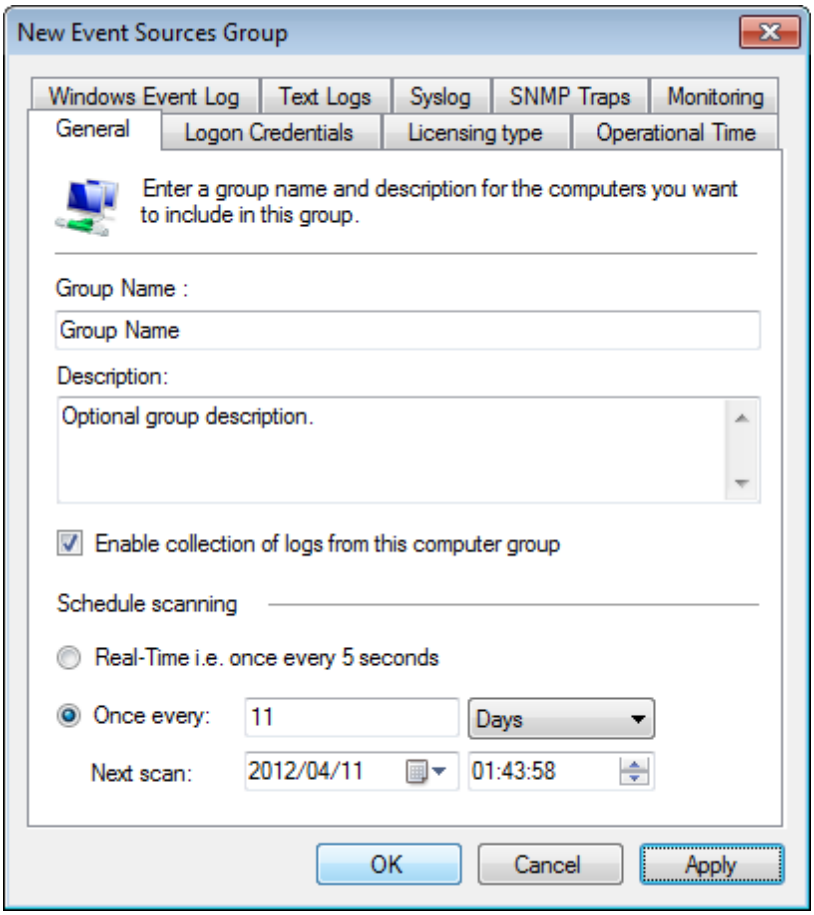
El agrupamiento de orígenes de eventos en grupos de orígenes de eventos mejora la velocidad a la que se configuran los orígenes de eventos. Una vez que se haya configurado un grupo de orígenes de eventos, todos los miembros de ese grupo heredan la misma configuración.

Para crear un nuevo grupo de orígenes de eventos:

1. Haga clic en la ficha **Configuration > Event Sources** y en **Group Type**, seleccione **Event Sources Groups**.

2. Haga clic con el botón secundario en **All event sources** y seleccione **Create group...**.

3. Seleccione el tipo de licencia. Elija una licencia **Complete** o **Active Monitoring**. Para obtener más información, consulte Configurar tipo de licencia de los orígenes de eventos.



Captura de pantalla 44: Agregar un nuevo grupo de orígenes de eventos

4. Ingrese un nombre único y una descripción opcional. Seleccione las fichas que se describen a continuación y configure las opciones disponibles:

Tabla 17: Opciones de grupo de orígenes de eventos

Nombre de la ficha	Description
General	Habilita la recopilación de eventos y programa el proceso de análisis. Para obtener más información, consulte Configurar propiedades generales de los orígenes de eventos.
Logon credentials	Permite configurar el nombre de usuario y la contraseña que se utilizan para iniciar sesión en equipos de destino y recopilar información. Para obtener más información, consulte Configurar credenciales de inicio de sesión de los orígenes de evento.
Licensing type	Permite seleccionar el tipo de licencia que se usará. Seleccione **Active Monitoring** o **Complete**. Para obtener más información, consulte Configurar tipo de licencia de los orígenes de eventos.
Operational time	Permite configurar el tiempo operativo en el que los equipos se utilizan normalmente. Para obtener más información, consulte Configurar tiempo operativo de los orígenes de eventos.
Monitoring	Permite habilitar la supervisión activa de GFI EventsManager en los equipos de destino y configurar las auditorías que se desean realizar. Las comprobaciones de supervisión permiten a los administradores identificar problemas del sistema en las primeras etapas para evitar tiempos de inactividad. Para obtener más información, consulte Configurar supervisión de los orígenes de eventos.
Windows Event Log	Permite especificar los registros que se desean recopilar y configurar los parámetros de almacenamiento de los registros de eventos de Windows®. Para obtener más información, consulte Recopilar eventos de Windows®.

Nombre de la ficha	Description
Text Logs	Permite especificar los registros que se desean recopilar y configurar los parámetros de los registros de W3C/HTTP/CSV. Esta ficha solamente está disponible cuando se crea un grupo de servidores. Para obtener más información, consulte Recopilar registros de texto.
Syslog	Permite especificar los registros que se desean recopilar y configurar los parámetros de almacenamiento para Syslogs. Esta ficha solamente está disponible cuando se crea un grupo de servidores. Para obtener más información, consulte Recopilar Syslogs.
SNMP Traps	Permite especificar los registros que se desean recopilar y configurar los parámetros de almacenamiento de capturas SNMP. Esta ficha solamente está disponible cuando se crea un grupo de servidores. Para obtener más información, consulte Recopilar capturas SNMP.

5. Haga clic en **Apply** y **OK**.

4.4 Configurar propiedades de orígenes de eventos

GFI EventsManager le permite personalizar los parámetros de orígenes de eventos para adaptarse a los requisitos de funcionamiento de su infraestructura. Puede configurar estos parámetros en cada origen de eventos o en un grupo de orígenes de eventos. Cualquier miembro de un grupo configurado hereda la misma configuración de forma automática.

Esta sección contiene información acerca de:

- Configurar propiedades generales de los orígenes de eventos
- Configurar credenciales de inicio de sesión de los orígenes de eventos
- Configurar tipo de licencia de los orígenes de eventos
- Configurar tiempo operativo de los orígenes de eventos
- Configurar supervisión de los orígenes de eventos
- Configurar parámetros de procesamiento de eventos

4.4.1 Configurar propiedades generales de orígenes de eventos

Utilice la ficha **General** del cuadro de diálogo de propiedades para:

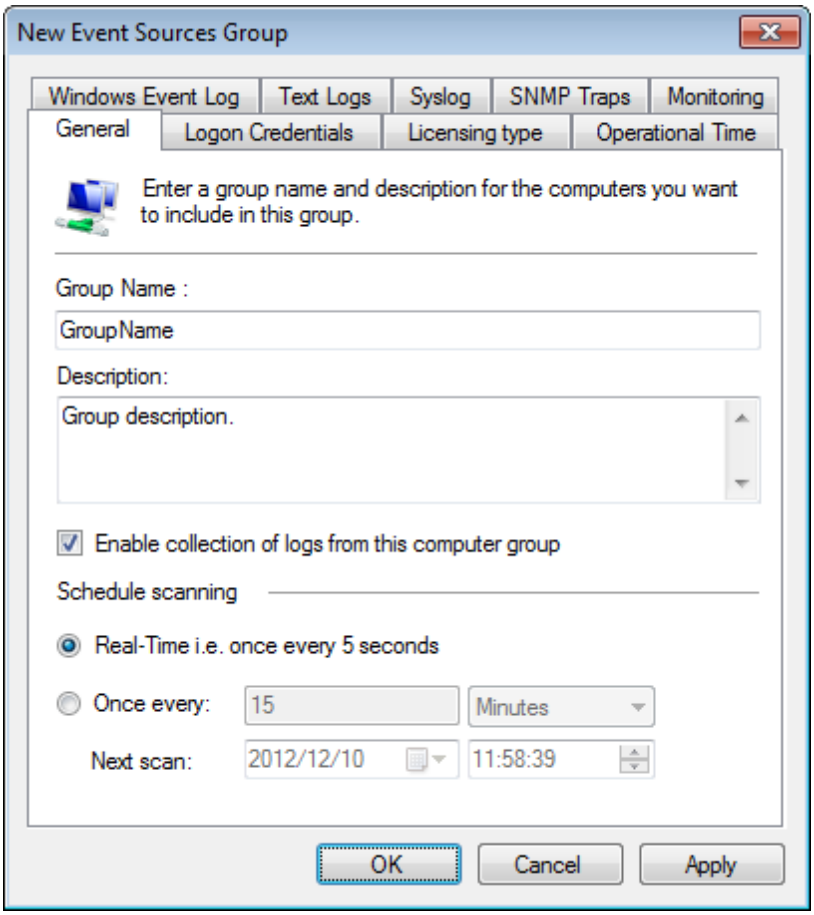
- Cambiar el nombre de un grupo de equipos
- Habilitar o inhabilitar la recopilación de registros y el procesamiento de los equipos de un grupo
- Configurar la frecuencia de recopilación y procesamiento de registros

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.

2. Para configurar los parámetros de:

- **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**
- **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.



Captura de pantalla 45: Cuadro de diálogo de propiedades de orígenes de eventos

3. En la ficha **General**, configure las opciones descritas a continuación:

Tabla 18: Propiedades de orígenes de eventos - Opciones generales

Opción	Descripción
Group Name	Ingrese un nombre exclusivo para el grupo de equipos.
Description	(Opcional) Escriba una descripción.
Enable collection of logs from this computer group	Marque o desmarque esta opción para habilitar o inhabilitar la recopilación de registros de eventos del grupo.
Real-Time i.e. once every 5 seconds	Seleccione esta opción para comprobar si hay nuevos registros de eventos cada 5 segundos. **Nota** Se recomienda si los miembros de este grupo generan grandes volúmenes de registros de eventos puesto que podría afectar el rendimiento de su red.
Once every	Especifique una programación personalizada para cuando GFI EventsManager busque nuevos registros de eventos.

4. Haga clic en **Apply** y **OK**.

4.4.2 Configurar credenciales de inicio de sesión de orígenes de eventos

Utilice la ficha **Logon Credentials** en el cuadro de diálogo de propiedades para:

- Ver la configuración de las credenciales de inicio de sesión
- Editar la configuración de las credenciales de inicio de sesión

Durante el procesamiento de eventos, GFI EventsManager debe iniciar sesión de forma remota en los equipos de destino. Esto es necesario con el fin de recopilar los datos de registro que se almacenan actualmente en los equipos de destino y pasar estos datos al motor de procesamiento de eventos.

Para recopilar y procesar los registros, GFI EventsManager debe tener privilegios administrativos en los equipos de destino. De forma predeterminada, GFI EventsManager inicia sesión en los equipos de destino utilizando las credenciales de la cuenta con la que se está ejecutando actualmente; sin embargo, algunos entornos de red están configurados para utilizar distintas credenciales para iniciar sesión en las estaciones de trabajo y servidores con privilegios administrativos.

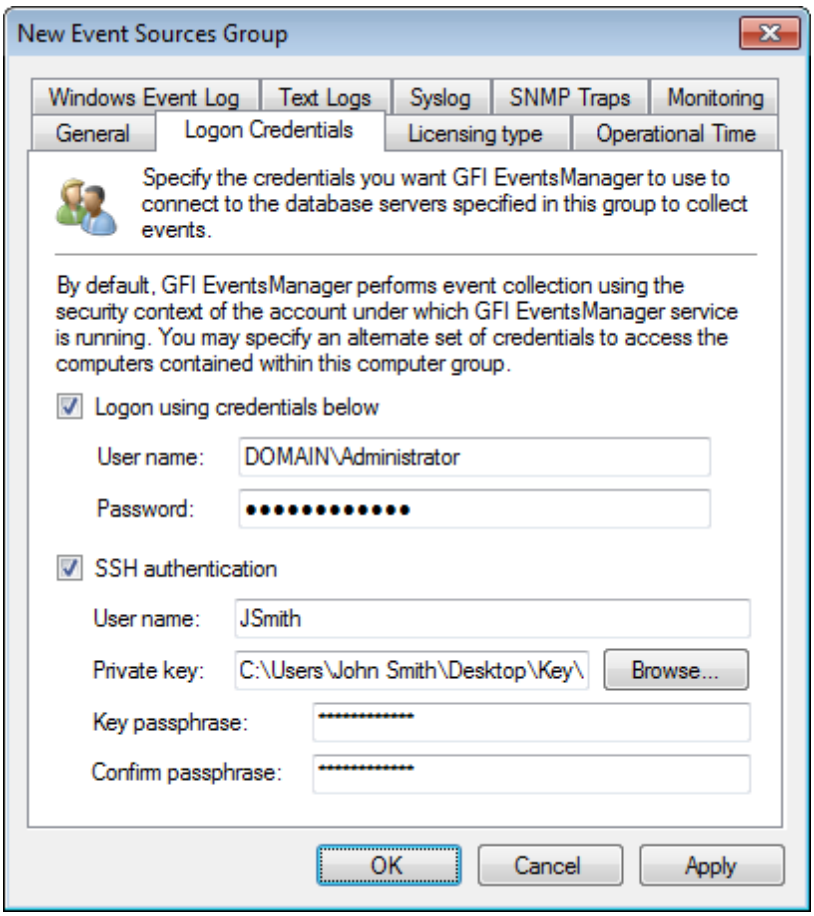
A modo de ejemplo, por motivos de seguridad, es posible que desee crear una cuenta de administrador que solamente tenga privilegios administrativos sobre las estaciones de trabajo y una cuenta diferente que únicamente tenga privilegios administrativos sobre los servidores.

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.

2. Para configurar los parámetros de:

- **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**
- **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.



Captura de pantalla 46: Configurar credenciales de inicio de sesión alternativas

3. Haga clic en la ficha **Logon Credentials**.

4. Marque o desmarque la opción **Logon using credentials below** para utilizar/dejar de utilizar las credenciales de inicio de sesión alternativas. Escriba un nombre de usuario y una contraseña.

Nota

Las credenciales de inicio de sesión alternativas le permiten utilizar diferentes nombres de usuario y contraseñas para iniciar sesión en equipos remotos. Puede configurar credenciales alternativas para un grupo de orígenes de eventos o para cada origen de evento.

Los miembros de un grupo de orígenes de eventos se pueden configurar para heredar credenciales del grupo primario.

5. Marque o desmarque la opción **SSH authentication** para utilizar/dejar de utilizar la autenticación SSH.

Nota

SSH utiliza criptografía de clave pública para autenticar el equipo remoto y permitirle autenticar al usuario, si es necesario. Se trata de un protocolo de seguridad para los equipos basados en Linux y Unix.

6. Haga clic en **Browse...** para seleccionar el archivo de **Private key**.

7. Ingrese la **clave de contraseña** y vuelva a escribirla para confirmarla.

8. Haga clic en **Apply** y **OK**.

4.4.3 Configurar el tipo de licencia de los orígenes de eventos

La ficha **Licensing type** se utiliza para configurar el modo de licencia de un origen de evento o grupo de eventos. Esto determina el tipo de registros que se deben recopilar del origen/grupo configurado. En la siguiente tabla, se describen los tipos de licencia disponibles:

Tabla 19: Tipos de licencia

Tipo de licencia	Descripción
Active Monitoring license	Esta licencia permite recopilar y procesar: » Registros de eventos de Microsoft®Windows® » Registros de texto, como W3C, CSV, XML, DHCP, registros SAP, registros SKIDATA y registros personalizados de estaciones de trabajo de Windows® o que no son de Windows®. » Registros de eventos de supervisión activa Si se detecta Windows® Server en un origen con esta licencia, el procesamiento de registros de eventos se inhabilita.

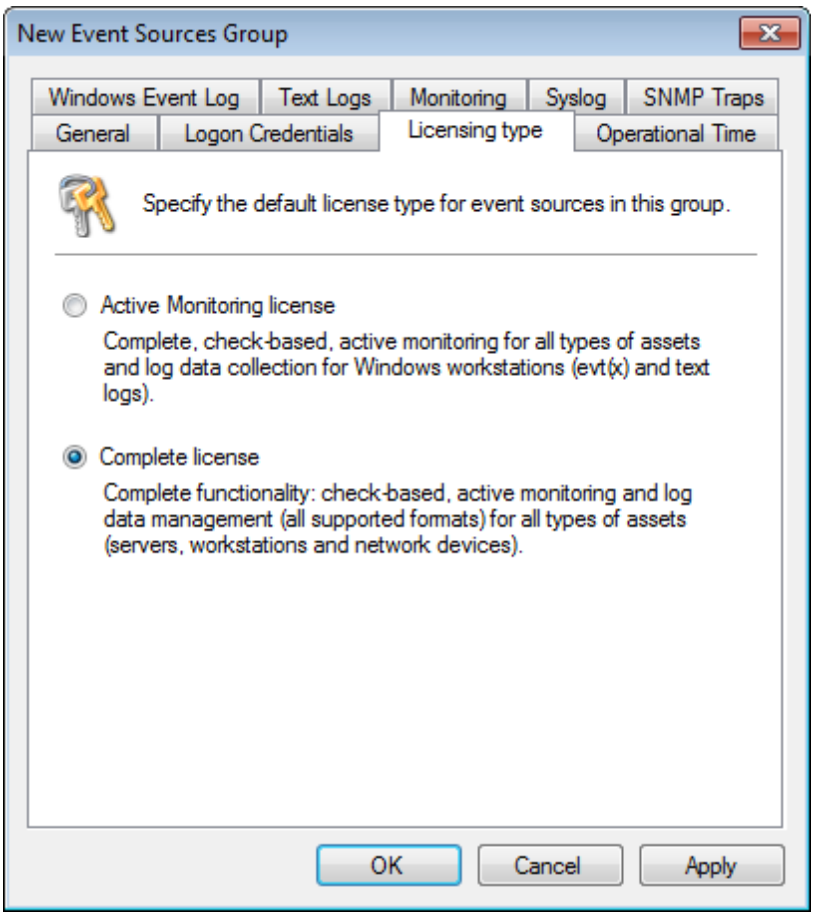
Tipo de licencia	Descripción
Complete license	Habilita funcionalidad y soporte integrales para servidores, estaciones de trabajo y dispositivos de red de Windows® y que no son de Windows®. Use esta licencia para recopilar y procesar: » Registros de eventos de Microsoft®Windows® » Registros de texto, como W3C, CSV, XML, DHCP, registros SAP, registros SKIDATA y registros personalizados de estaciones de trabajo de Windows® o que no son de Windows®. » Registros de eventos de supervisión activa » Mensajes de captura SNMP » Syslogs » Registros personalizados » Auditorías SQL Server® » Auditorías de Oracle Server

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.
2. Para configurar los parámetros de:

» **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**

» **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.


New Event Sources Group
Windows Event Log
Text Logs
Monitoring
Syslog
SNMP Traps
General
Logon Credentials
Licensing type
Operational Time
Specify the default license type for event sources in this group.
Active Monitoring license
Complete, check-based, active monitoring for all types of assets and log data collection for Windows workstations (evt(x) and text logs).
Complete license
Complete functionality: check-based, active monitoring and log data management (all supported formats) for all types of assets (servers, workstations and network devices).
OK
Cancel
Apply

Captura de pantalla 47: Configurar el tipo de licencia de los orígenes de eventos

3. Haga clic en la ficha **Licensing type** y seleccione la licencia que desee utilizar para el origen del evento o grupo que se esté configurando.

4. Haga clic en **Apply** y **OK**.

4.4.4 Configurar el tiempo operativo de los orígenes de eventos

GFI EventsManager incluye una opción de tiempo operativo a través de la cual se especifican las horas normales de trabajo de sus grupos de orígenes de eventos. Esto es necesario para que GFI EventsManager pueda realizar un seguimiento de los eventos que ocurren durante las horas laborales y no laborales.

Utilice la información de tiempo operativo para el análisis forense; para identificar el acceso de usuarios no autorizados, transacciones ilícitas realizadas fuera de las horas normales de trabajo y otras infracciones de seguridad potenciales que se podrían estar llevando a cabo en la red.

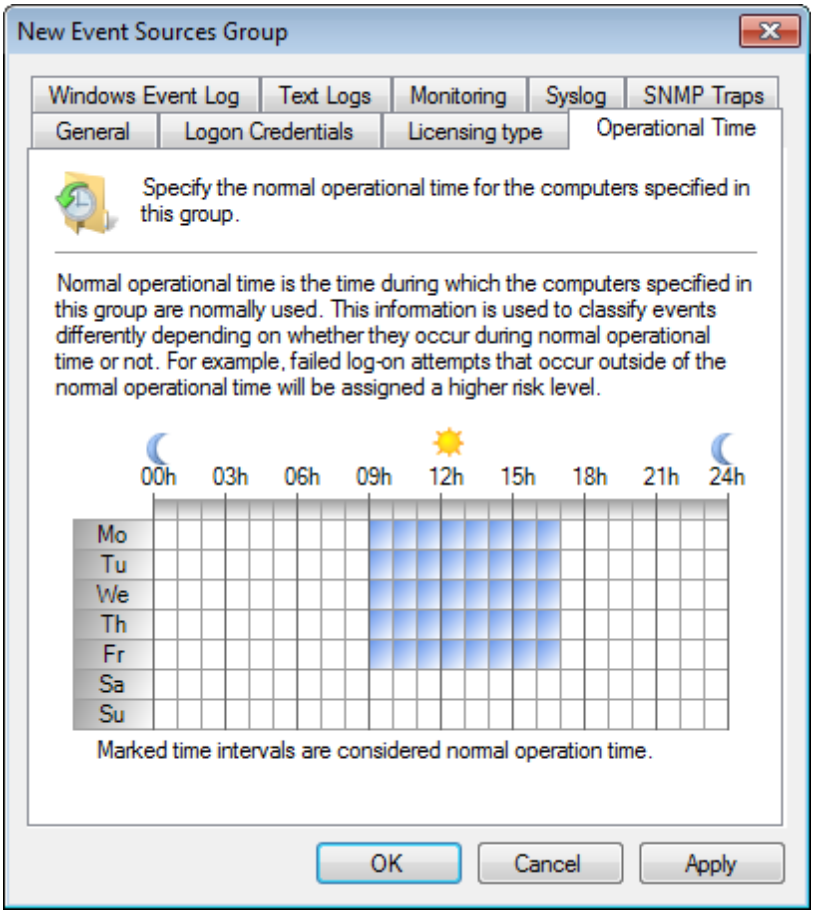
El tiempo operativo se puede configurar en base a un grupo de equipos. Esto se logra al marcar las horas de trabajo normales en una escala gráfica de tiempo operativo que se divide en segmentos de una hora.

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.

2. Para configurar los parámetros de:

- **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**
- **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.



Captura de pantalla 48: Especificar tiempo operativo

3. En la ficha **Operational Time**, marque los intervalos de tiempo de sus horas normales de trabajo.

> **Nota**
>
> Las celdas marcadas en azul representan sus horas normales de trabajo.

4. Haga clic en **Apply** y **OK**.

4.4.5 Configurar la supervisión de orígenes de eventos

GFI EventsManager es capaz de recopilar información adicional acerca de sus orígenes de eventos a través de la supervisión activa. Estas comprobaciones generan eventos específicos que, a su vez, activan notificaciones en tiempo real o ejecutan una acción.

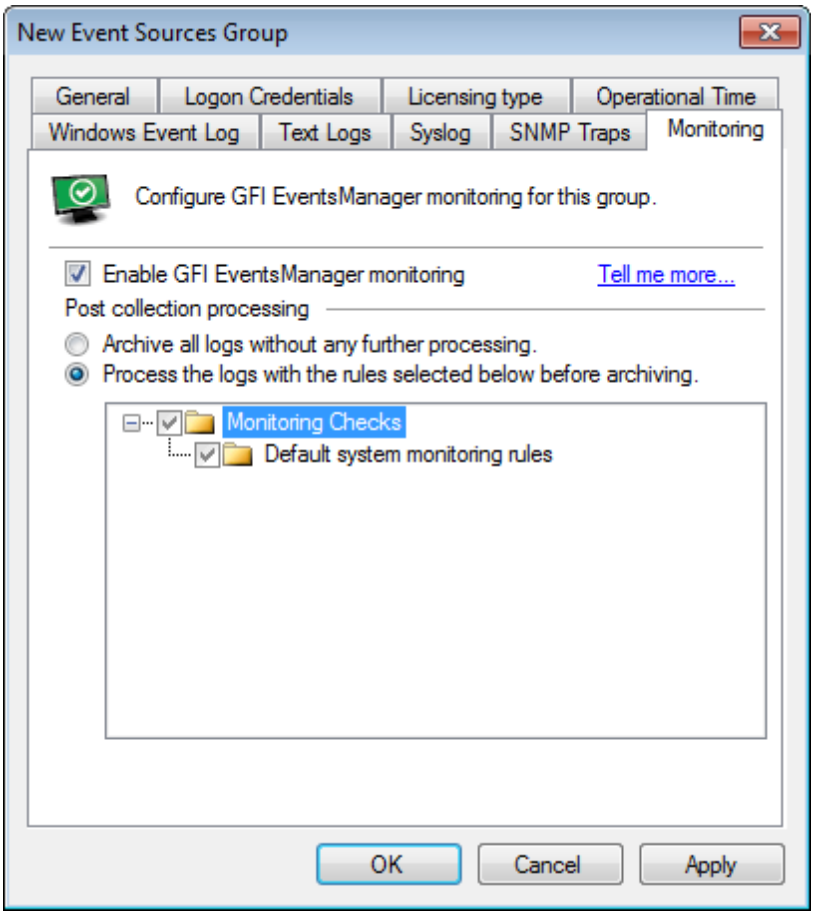
Por ejemplo, cuando se supervisa la comprobación del **uso de CPU**, GFI EventsManager consulta ese origen de evento y detecta si el equipo de destino está funcionando según los niveles de uso de CPU especificados.

> **Nota**
>
> Para obtener más información, consulte Supervisión activa.

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.
2. Para configurar los parámetros de:

- **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**
- **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.



Captura de pantalla 49: Ficha Event source properties - Monitoring

3. En la ficha **Monitoring**, configure las opciones descritas a continuación:

Tabla 20: Opciones de supervisión de orígenes de eventos

Opción	Descripción
Inherit event log collection and processing from parent group	Esta opción está disponible cuando se habilita la supervisión de un único origen de evento. Si habilitó la supervisión en el grupo que contiene el origen del evento, marque esta opción para obtener la misma configuración.
Enable GFI EventsManager monitoring	Marque o desmarque esta opción para habilitar o inhabilitar el procesamiento de la supervisión activa.
Perform the following checks	Expanda la lista de comprobaciones y seleccione las que desea aplicar a su origen de evento/grupo de orígenes de eventos. Para obtener información sobre la creación de comprobaciones de supervisión, consulte Crear una nueva comprobación de supervisión.
Archive all logs without any further processing	Seleccione esta opción para almacenar los eventos sin aplicar ninguna otra comprobación (en Events Processing Rules).
Process the logs with the rules selected below before archiving	Expanda la lista de reglas que se aplican a los registros recopilados. GFI EventsManager le permite crear reglas personalizadas y configurarlas para activarlas cuando una de las comprobaciones de supervisión genera un evento. A continuación, a través de la configuración de la regla de procesamiento de eventos seleccionada, se ejecutan acciones o se generan alertas. Una vez que una comprobación de supervisión está habilitada, busque el evento que genera y cree una regla basada en ese evento. Para obtener más información, consulte Crear nuevas reglas desde eventos existentes.

4. Haga clic en **Apply** y **OK**.

4.4.6 Configurar parámetros de procesamiento de eventos

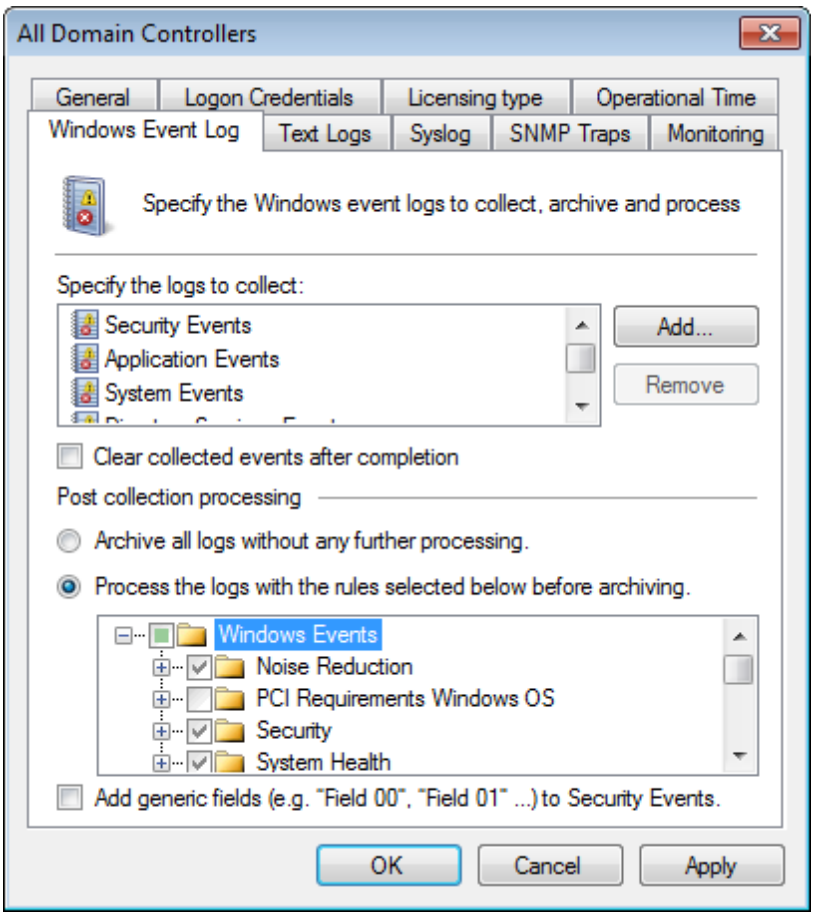
La configuración del procesamiento de eventos está habilitada solamente para orígenes/grupos con licencia de servidores. Los orígenes de eventos del servidor tienen más opciones de configuración que las estaciones de trabajo normales, con el fin de recopilar registros de eventos, registros de texto, Syslogs y capturas SNMP de Windows®.

Para configurar las propiedades de los orígenes de eventos:

1. En la ficha **Configuration > Event Sources > Group Type**, seleccione **Event Sources Groups**.

2. Para configurar los parámetros de:

- **Computer group**: haga clic con el botón secundario en el grupo de equipos que desea configurar y seleccione **Properties**
- **Single event source**: haga clic con el botón secundario en el origen que desea configurar y seleccione **Properties**.



Captura de pantalla 50: Fichas de configuración de procesamiento de eventos

3. Utilice las fichas **Windows Event Log**, **Text Logs**, **Syslog** y **SNMP Traps** para configurar los parámetros de procesamiento de eventos requeridos.

4. Haga clic en **Apply** y en **OK**.

Nota

Para obtener más información, consulte:

- Recopilar registros de eventos de Windows®
- Recopilar registros de texto
- Recopilar Syslogs
- Recopilar capturas SNMP

4.5 Orígenes de bases de datos

GFI EventsManager puede supervisar y procesar eventos desde servidores de bases de datos. Los orígenes de eventos de bases de datos requieren parámetros de configuración específicos para recopilar y procesar los eventos generados por la actividad de la base de datos. GFI EventsManager es capaz de auditar y supervisar la actividad de los siguientes servidores de bases de datos:

- Microsoft® SQL Server®
- Oracle Server

4.5.1 Orígenes de Microsoft®SQL Server®

Esta sección contiene información acerca de:

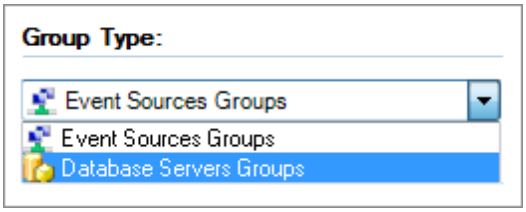
- Crear un nuevo grupo de Microsoft® SQL Server®
- Agregar un nuevo origen de eventos de Microsoft® SQL Server®

Crear un nuevo grupo de Microsoft®SQL Server®

Para crear un grupo de Microsoft® SQL Server®:

1. Haga clic en la ficha **Configuration > Event Sources**.

2. En **Group Type**, seleccione **Database Servers Groups**.



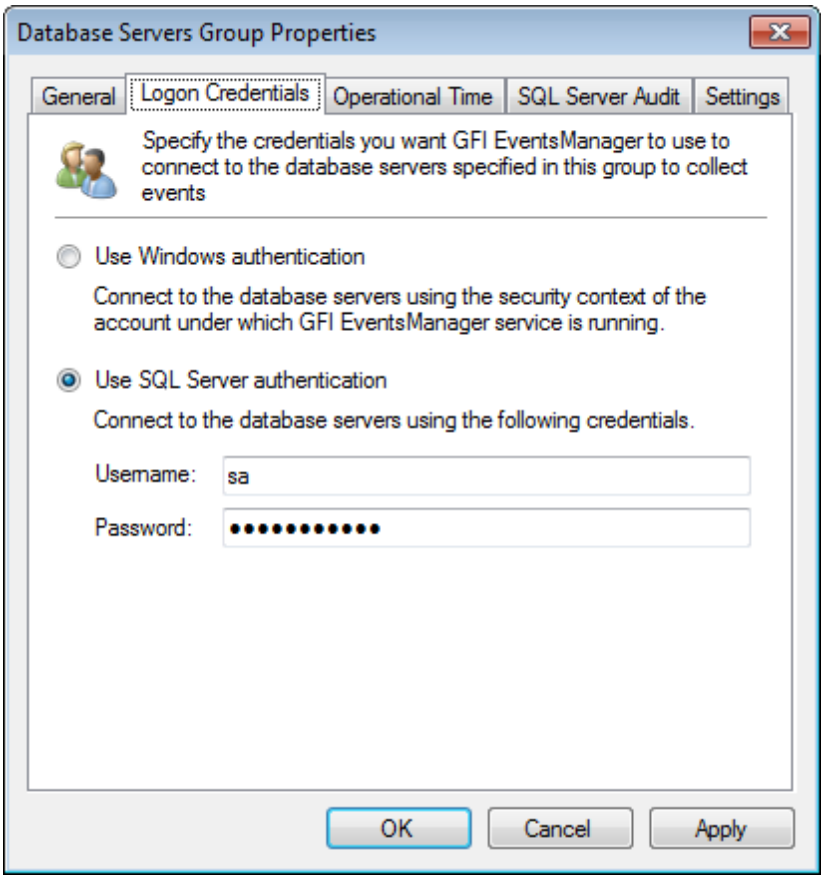
Captura de pantalla 51: Grupos de servidores de base de datos

3. En **Groups**, haga clic con el botón secundario en **Microsoft®SQL Server®** y seleccione **Create group...**.

4. Seleccione **Microsoft®SQL Server®** como tipo de servidor y en la ficha **General** configure las opciones descritas a continuación:

Tabla 21: Grupo de base de datos de Microsoft® SQL: General

Opción	Description
Group Name	Ingrese un nombre de grupo para identificar el grupo de Microsoft® SQL Server®.
Description	(Opcional) Escriba una descripción.
Collects logs from the database servers included in this group	Permite habilitar la opción para recopilar eventos de base de datos de todos los servidores de este grupo.

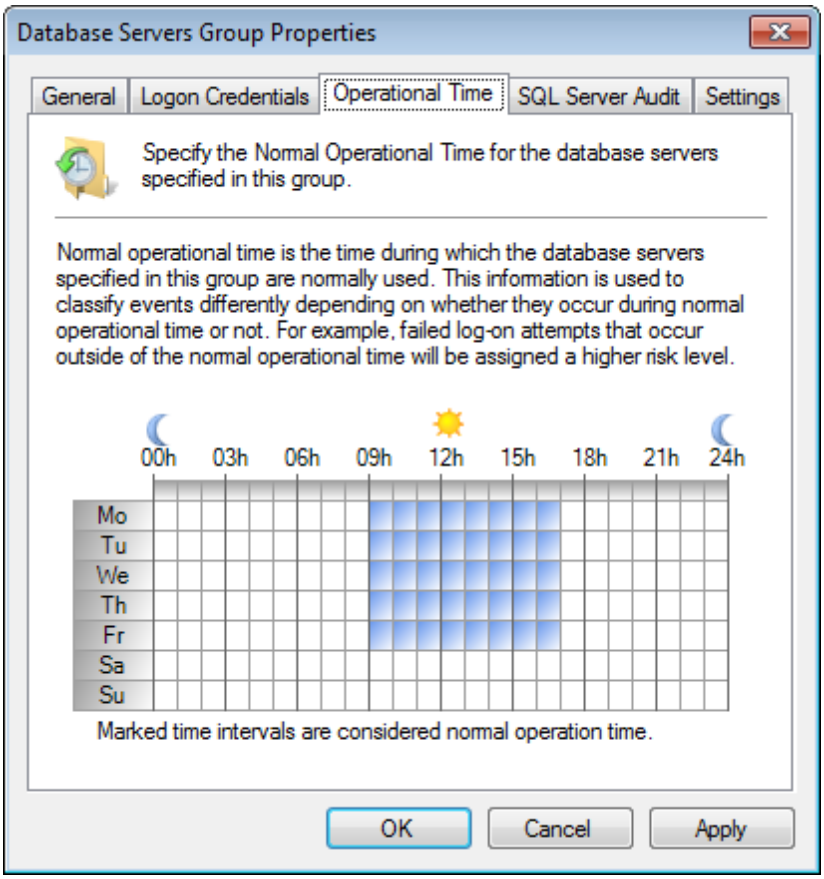

Database Servers Group Properties
General
Logon Credentials
Operational Time
SQL Server Audit
Settings
Specify the credentials you want GFI EventsManager to use to connect to the database servers specified in this group to collect events
Use Windows authentication
Connect to the database servers using the security context of the account under which GFI EventsManager service is running.
Use SQL Server authentication
Connect to the database servers using the following credentials.
Username:
sa
Password:
OK
Cancel
Apply

Captura de pantalla 52: Configurar parámetros de inicio de sesión en la ficha Logon Credentials

4. Seleccione la ficha **Logon Credentials** y configure las opciones que se describen a continuación:

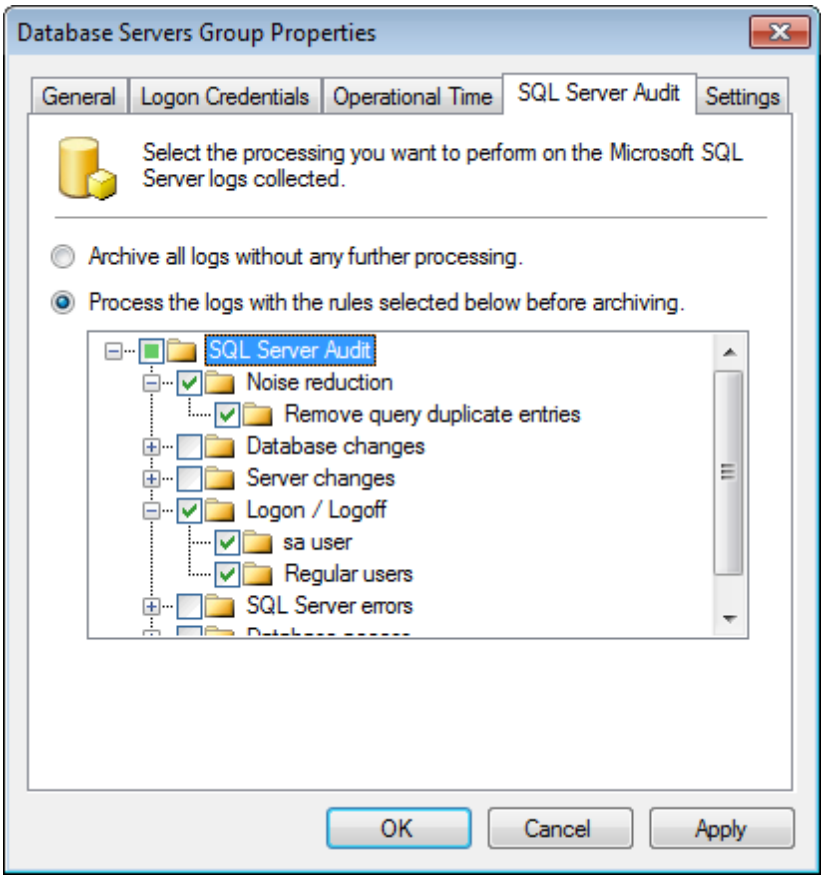
Tabla 22: Grupo de base de datos de Microsoft® SQL: Credenciales de inicio de sesión

Opción	Descripción
Use Windows authentication	Permite conectarse a la base de datos de Microsoft® SQL mediante la autenticación de Windows.
Use SQL Server® authentication	Permite conectarse a la base de datos de Microsoft® SQL a través de una cuenta de usuario de la base de datos de Microsoft® SQL. Escriba un nombre de usuario y una contraseña.



Captura de pantalla 53: Configurar horas normales de trabajo de la ficha Operational Time

5. Seleccione **Operational Time** y configure el tiempo operativo en el que se utiliza normalmente la base de datos. Los intervalos de tiempo marcados se consideran horas normales de trabajo.

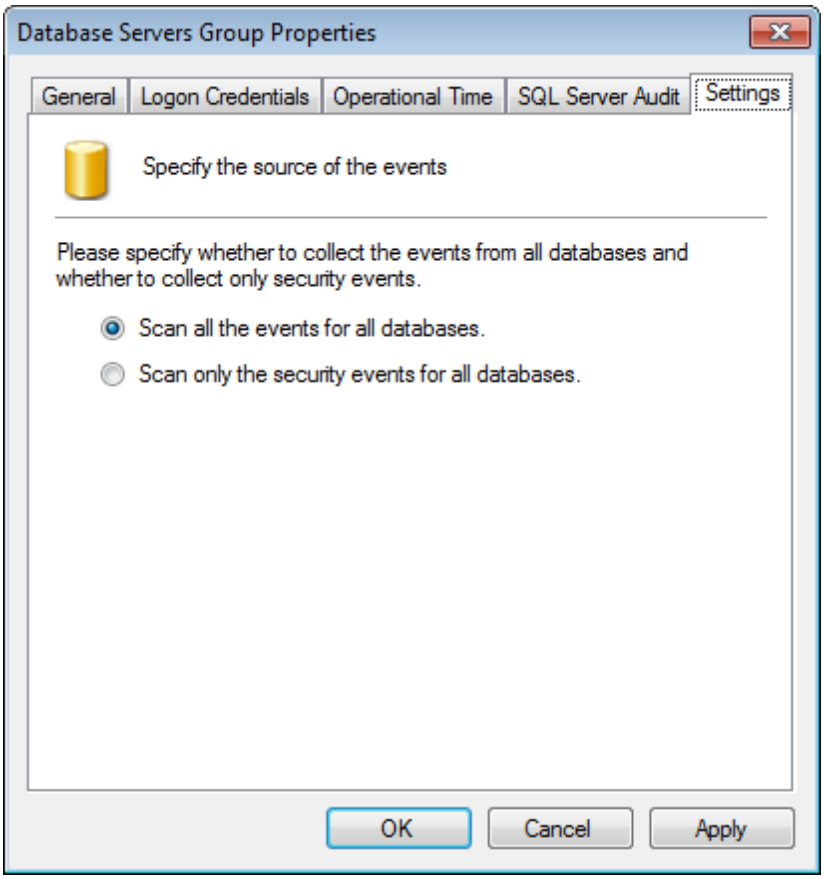


Captura de pantalla 54: Configurar auditoría de SQL Server en la ficha SQL Server Audit

6. Seleccione la ficha **SQL Server®Audit** y configure las opciones que se describen a continuación:

Tabla 23: Grupo de base de datos de Microsoft® SQL - SQL Server® Auditoría

Opción	Descripción
Archive all logs without further processing	Permite archivar eventos en el back-end de la base de datos de GFI EventsManager sin aplicar reglas de procesamiento.
Process the logs with the rules selected below before archiving	Permite especificar las reglas que desea ejecutar antes de archivar eventos en el back-end de la base de datos de GFI EventsManager.


Database Servers Group Properties
General
Logon Credentials
Operational Time
SQL Server Audit
Settings
Specify the source of the events
Please specify whether to collect the events from all databases and whether to collect only security events.
Scan all the events for all databases.
Scan only the security events for all databases.
OK
Cancel
Apply

7. Seleccione la ficha **Settings** y configure las opciones descritas a continuación:

Tabla 24: Grupo de base de datos de Microsoft® SQL - Configuración

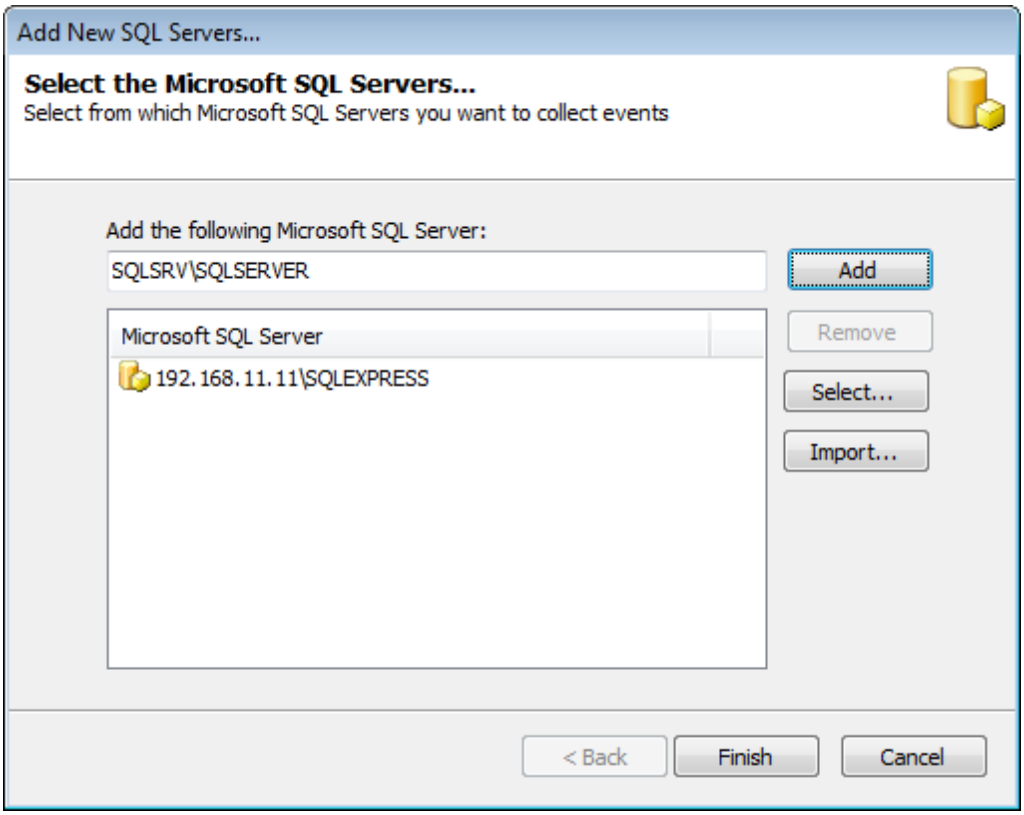
Opción	Descripción
Scan all the events for all databases	Todos los eventos de Microsoft® SQL Server® son recopilados y procesados por GFI EventsManager.
Scan only security events for all databases	Solamente los eventos de seguridad son recopilados y procesados por GFI EventsManager.

8. Haga clic en **Aplicar** y **Aceptar**.

Agregar un nuevo origen de eventos de Microsoft® SQL Server®

Para agregar un nuevo origen de Microsoft® SQL Server®:

1. Haga clic con el botón secundario en un grupo de base de datos y seleccione **Add newSQL Server®...**.



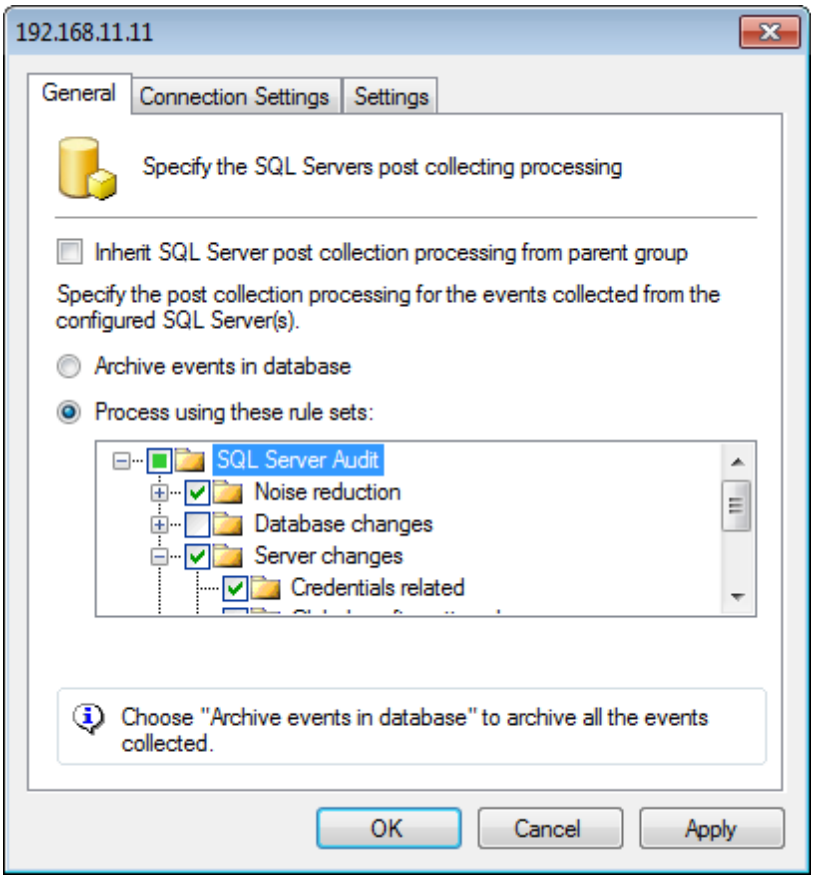
Captura de pantalla 55: Agregar nuevo servidor de Microsoft® SQL

2. Escriba el nombre del servidor o la dirección IP y haga clic en **Add**.

> **Nota**
>
> Use **Select** e **Import** para buscar en la red de SQL Server® o importar una lista de servidores SQL desde un archivo de texto, respectivamente.

3. Haga clic en **Finish**; se cierra el cuadro de diálogo Add New SQL Servers.

4. En **Groups**, seleccione **SQL Servers** y, en el panel derecho, haga doble clic en la nueva instancia de base de datos de Microsoft® SQL.

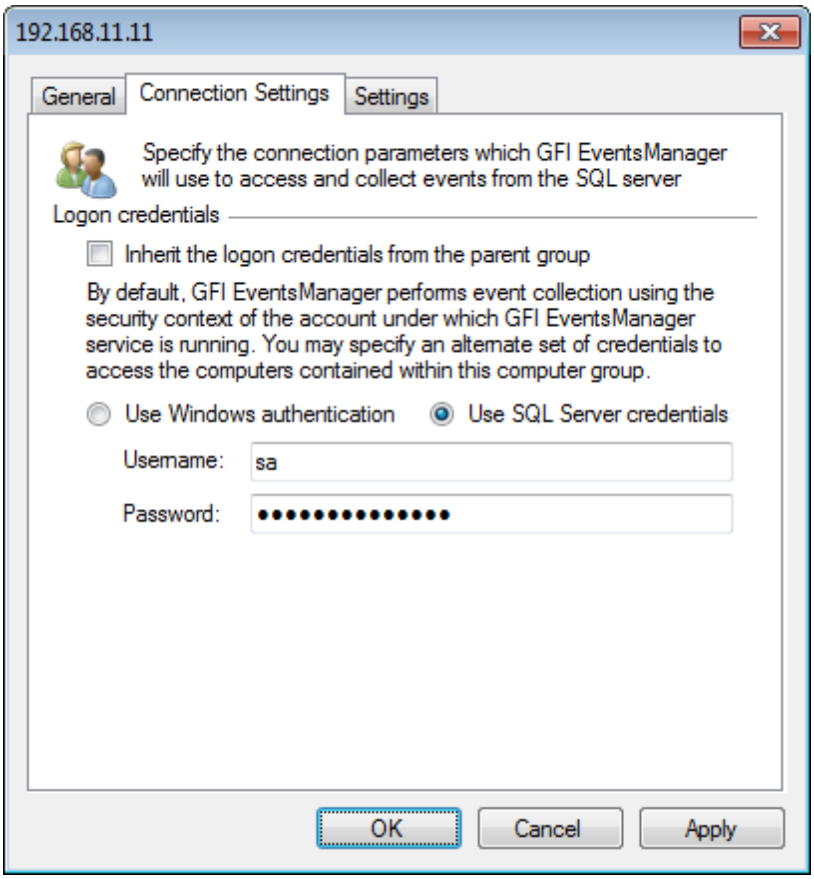


Captura de pantalla 56: Propiedades de la base de datos de Microsoft® SQL: Ficha General

5. En la ficha **General**, configure las opciones que se describen a continuación:

Tabla 25: Base de datos de Microsoft® SQL - Opciones de la ficha General

Opción	Descripción
Inherit SQL Server post collecting processing from parent group	Hereda toda la configuración del grupo primario.
Archive events in database	Permite archivar eventos en el back-end de la base de datos de GFI EventsManager sin aplicar reglas de procesamiento.
Process using these rule sets	Permite especificar las reglas que desea ejecutar antes de archivar eventos en el back-end de la base de datos de GFI EventsManager.

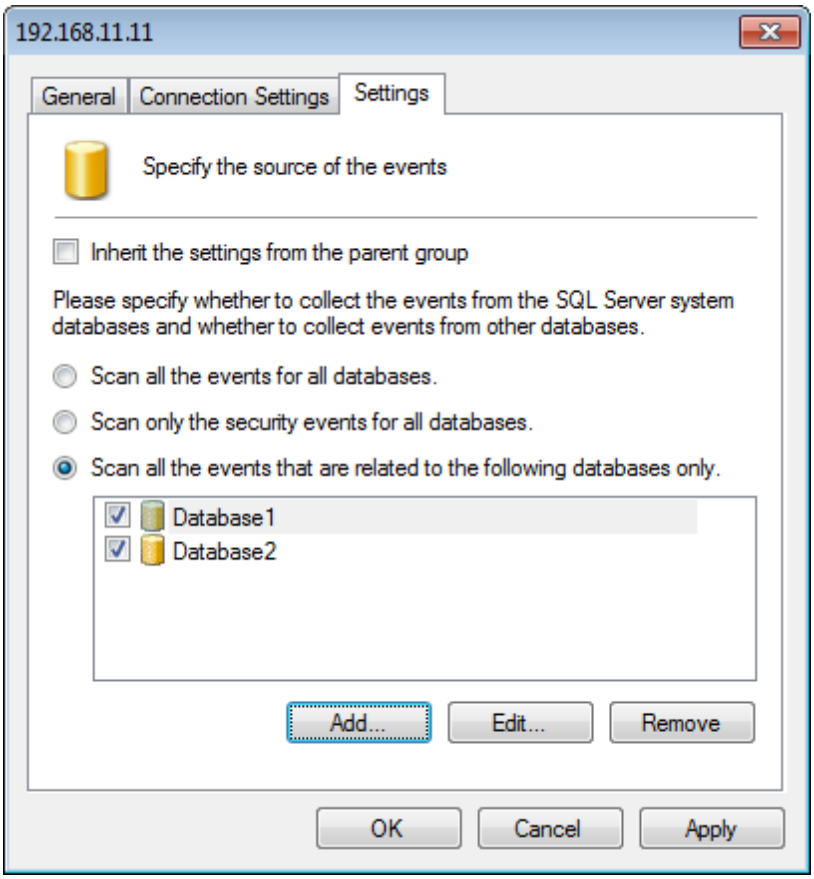

192.168.11.11
General
Connection Settings
Settings
Specify the connection parameters which GFI EventsManager will use to access and collect events from the SQL server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Use Windows authentication
Use SQL Server credentials
Username:
sa
Password:
OK
Cancel
Apply

Captura de pantalla 57: Propiedades de la base de datos de Microsoft® SQL: Ficha Connection Settings

6. Seleccione **Connection Settings** y configure las opciones que se describen a continuación:

Tabla 26: Base de datos de Microsoft® SQL - Ficha Connection Settings

Opción	Descripción
Inherit the logon credentials from the parent group	Seleccione esta opción para heredar la configuración de inicio de sesión del grupo primario.
Use Windows authentication	Permite conectarse con la base de datos de Microsoft® SQL mediante la autenticación de Windows.
Use SQL Server credentials	Permite conectarse a la base de datos de Microsoft® SQL a través de una cuenta de usuario de la base de datos de Microsoft® SQL. Escriba un nombre de usuario y una contraseña.


192.168.11.11
General
Connection Settings
Settings
Specify the source of the events
Inherit the settings from the parent group
Please specify whether to collect the events from the SQL Server system databases and whether to collect events from other databases.
Scan all the events for all databases.
Scan only the security events for all databases.
Scan all the events that are related to the following databases only.
Database1
Database2
Add...
Edit...
Remove
OK
Cancel
Apply

Captura de pantalla 58: Propiedades de la base de datos de Microsoft® SQL: Ficha Settings

7. Seleccione la ficha **Settings** y configure las opciones que se describen a continuación:

Tabla 27: Base de datos de Microsoft® SQL - Opciones de la ficha Settings

Opción	Descripción
Inherit the settings from the parent group	Hereda la configuración del grupo primario.
Scan all the events for all databases	Permite analizar todas las bases de datos y recopilar todos los eventos de Microsoft® SQL Server®.
Scan only the security events for all databases	Permite analizar todas las bases de datos y recopilar solamente los eventos de seguridad de Microsoft® SQL Server®.
Scan all the events that are related to the following databases only	Permite recopilar todos los eventos de las bases de datos seleccionadas. Utilice Add, Edit y Remove para administrar los orígenes de las bases de datos.

8. Haga clic en **Apply** y **OK**.

4.5.2 Orígenes de Oracle Server

GFI EventsManager le permite recopilar y procesar los eventos generados por los sistemas de administración de bases de datos de Oracle Relational. Las siguientes auditorías son recopiladas y procesadas por GFI EventsManager:

Tabla 28: Auditorías admitidas por Oracle Server

Auditoría	Descripción
Session auditing	Audita sesiones de usuarios y acceso a bases de datos.
Statement auditing	Audita declaraciones procesadas por SQL.
Object auditing	Audita consultas y declaraciones relacionadas con objetos específicos.

Las siguientes versiones de Oracle Database son admitidas:

- Oracle Database 9i
- Oracle Database 10g
- Oracle Database 11g

Esta sección contiene información acerca de:

- Parámetros previos a la configuración de orígenes de eventos de Oracle Server
- Crear nuevo grupo de Oracle Server
- Agregar nuevo origen de eventos de Oracle Server

Parámetros previos a la configuración de orígenes de eventos de Oracle Server

Antes de agregar orígenes de eventos de Oracle Server, siga estos pasos en cada instancia de Oracle Server que desee supervisar:

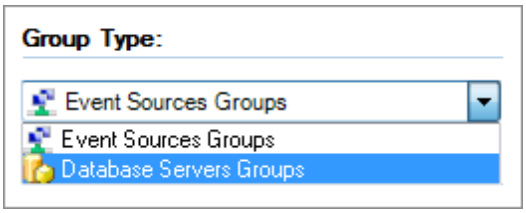
Tabla 29: Etapas de configuración de Oracle Server

Paso previo a la configuración	Descripción
Paso 1	Asegúrese de que las credenciales de inicio de sesión que se utilizan para conectarse, configurar auditorías y acceder a la tabla de auditoría tengan los permisos necesarios.
Paso 2	Habilite la auditoría en Oracle Server mediante el cambio de los parámetros de inicio. Para habilitar la auditoría: 1. Los parámetros de inicio para los servidores de Oracle se almacenan en: `<Oracle Home Directory>\admin\<Oracle SID>\pfile\init.ora.` 2. Busque y abra el archivo de parámetros utilizando un editor de texto. 3. Localice el parámetro **AUDIT_TRAIL** y cambie el valor predeterminado a '**db**' o '**db_extended**' ('db,extended' en las últimas versiones de Oracle). 4. Guarde y reinicie el servidor de Oracle.

Agregar nuevo grupo de Oracle Server

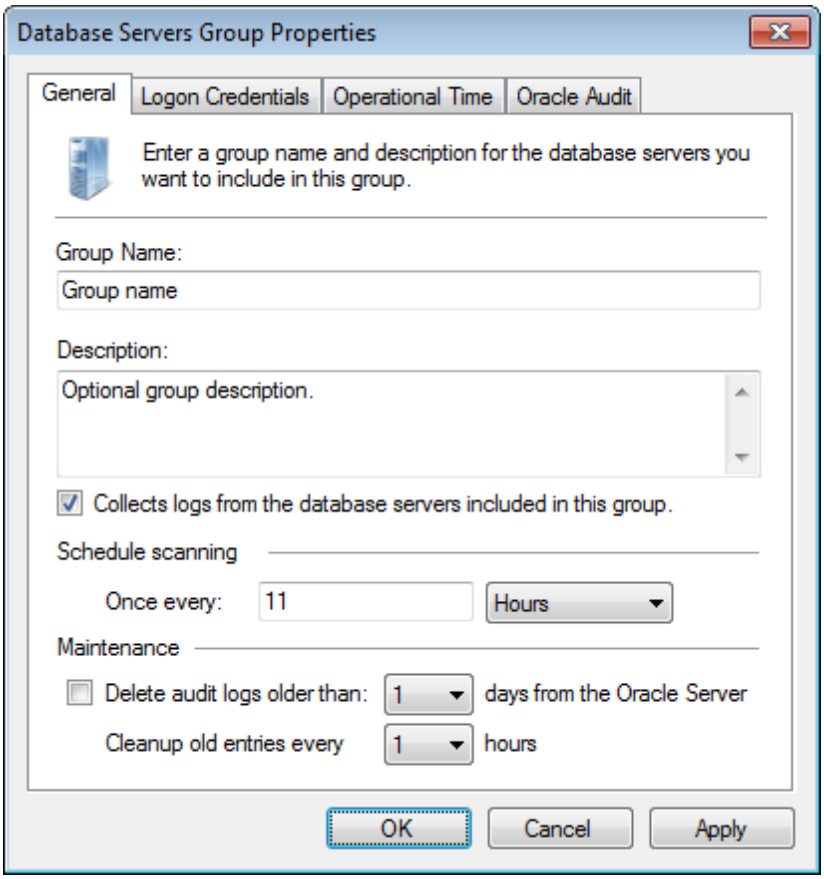
Para agregar un nuevo grupo de Oracle Database:

1. Haga clic en la ficha **Configuration > Event Sources**.
2. En **Group Type**, seleccione **Database Servers Groups**.



Captura de pantalla 59: Grupos de servidores de base de datos

3. En **Groups**, haga clic con el botón secundario en **Oracle Servers** y seleccione **Create group...**.

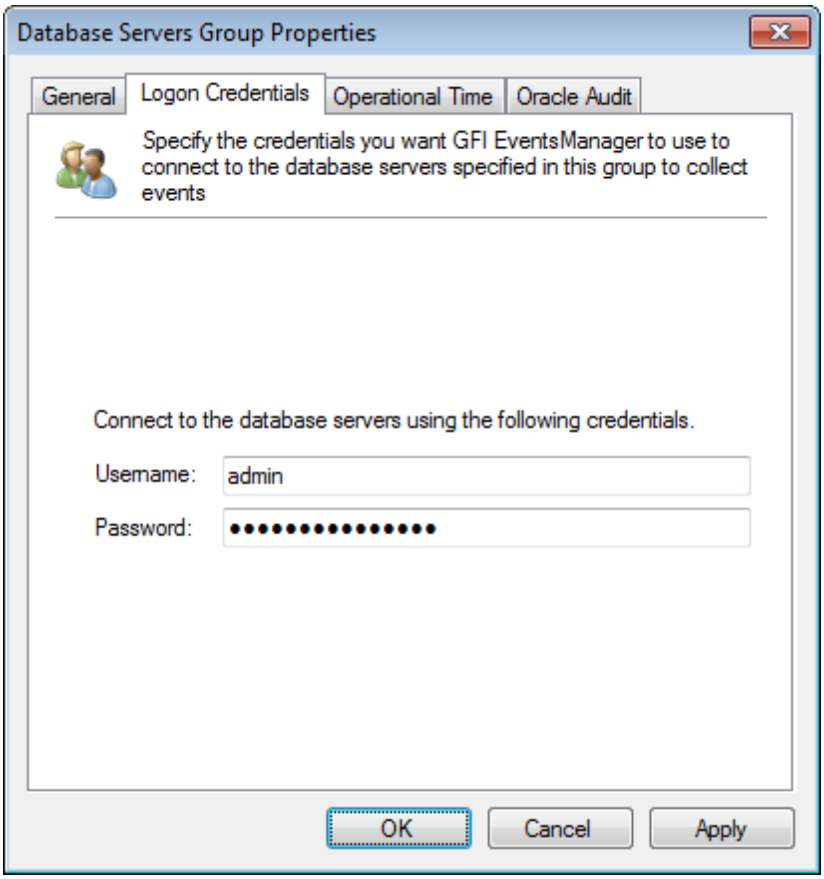


Captura de pantalla 60: Ficha Oracle Database group - General

4. En la ficha **General**, configure las opciones que se describen a continuación:

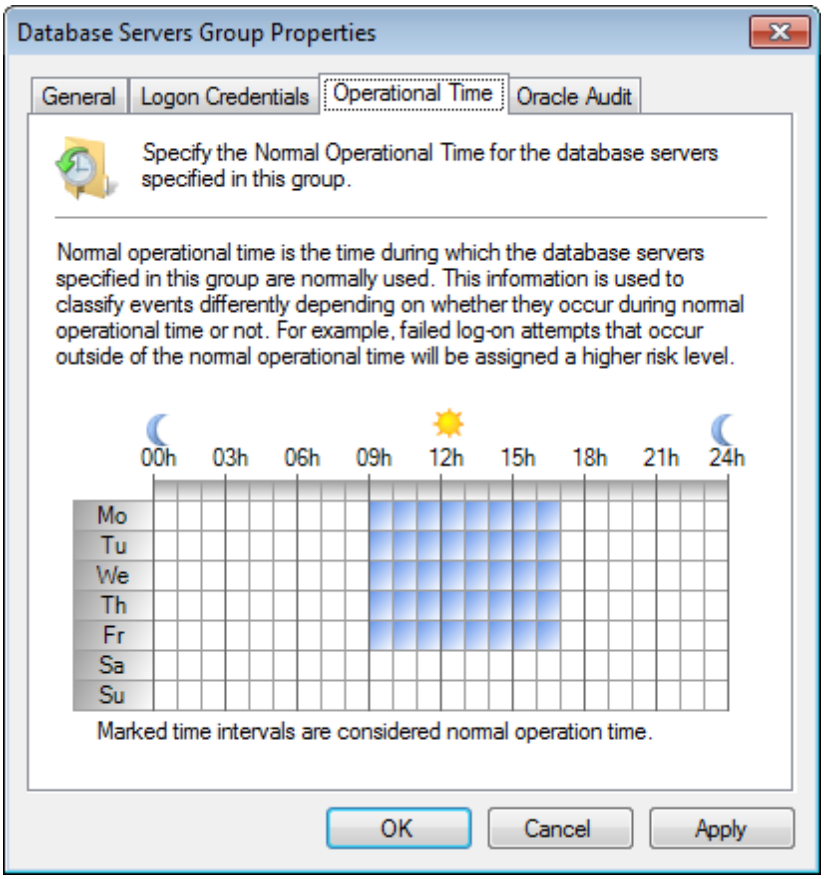
Tabla 30: Grupo de base de datos de Oracle- General

Opción	Descripción
Group Name	Ingrese un nombre de grupo para identificar el grupo de Oracle Server.
Description	Opcionalmente, ingrese una descripción.
Collects logs from the database servers included in this group	Permite recopilar eventos de los orígenes de eventos en el grupo de Oracle. Una vez que se habilita esta opción, configure las opciones de programación de análisis y mantenimiento.
Schedule scanning	Permite especificar la frecuencia para recopilar eventos en un horario predefinido.
Maintenance	Los eventos de auditoría de Oracle se almacenan en una tabla de auditoría específica en el servidor de Oracle. Para evitar el crecimiento excesivo de una tabla de auditoría, configure las opciones de esta sección para eliminar los registros de auditoría y entradas antiguas en un tiempo predefinido.



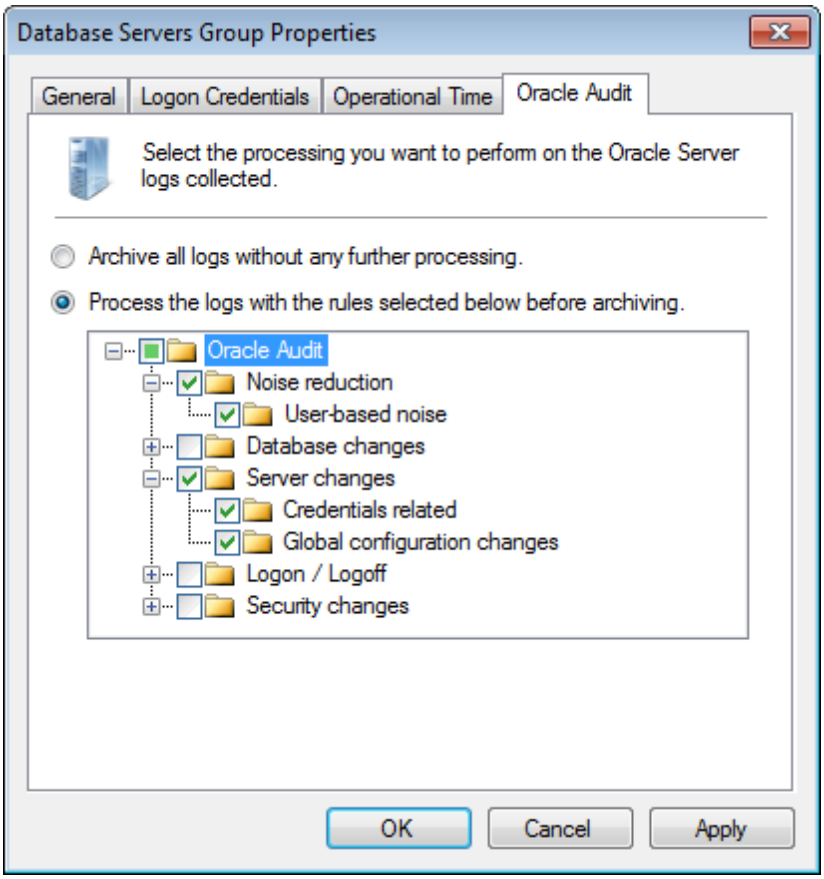
Captura de pantalla 61: Ficha Oracle Database group - Logon Credentials

5. Seleccione la ficha **Logon Credentials** e ingrese un nombre de usuario y una contraseña válidos para conectarse al servidor de Oracle.


Database Servers Group Properties
General
Logon Credentials
Operational Time
Oracle Audit
Specify the Normal Operational Time for the database servers specified in this group.
Normal operational time is the time during which the database servers specified in this group are normally used. This information is used to classify events differently depending on whether they occur during normal operational time or not. For example, failed log-on attempts that occur outside of the normal operational time will be assigned a higher risk level.
00h
03h
06h
09h
12h
15h
18h
21h
24h
Mo
Tu
We
Th
Fr
Sa
Su
Marked time intervals are considered normal operation time.
OK
Cancel
Apply

Captura de pantalla 62: Ficha Oracle Database group - Operational Time

6. Seleccione la ficha **Operational Time** y configure el tiempo operativo normal de los servidores de la base de datos de Oracle en este grupo.



Captura de pantalla 63: Ficha Oracle Database group - Oracle Audit

7. Seleccione **Oracle Audit** y configure las opciones que se describen a continuación:

Tabla 31: Grupo de base de datos de Oracle Database - Auditoría de Oracle

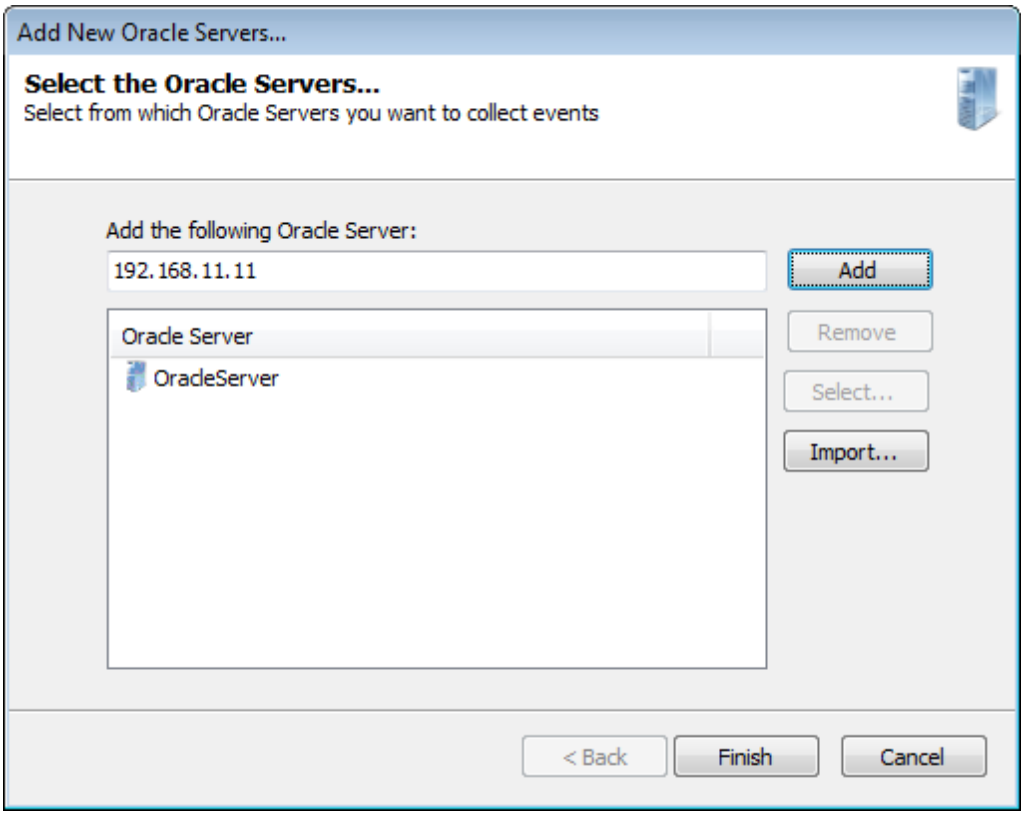
Opción	Description
Archive all logs without further processing	Permite archivar eventos en el back-end de la base de datos de GFI EventsManager sin aplicar reglas de procesamiento.
Process the logs with the rules selected below before archiving	Permite especificar las reglas que desea ejecutar antes de archivar eventos en el back-end de la base de datos de GFI EventsManager.

8. Haga clic en **Apply** y **OK**.

Agregar nuevo origen de eventos de Oracle Server

Para agregar una nueva base de datos de Oracle a un grupo de bases de datos:

1. Haga clic con el botón secundario en un grupo de Oracle Server y seleccione **Add new Oracle Server...**.



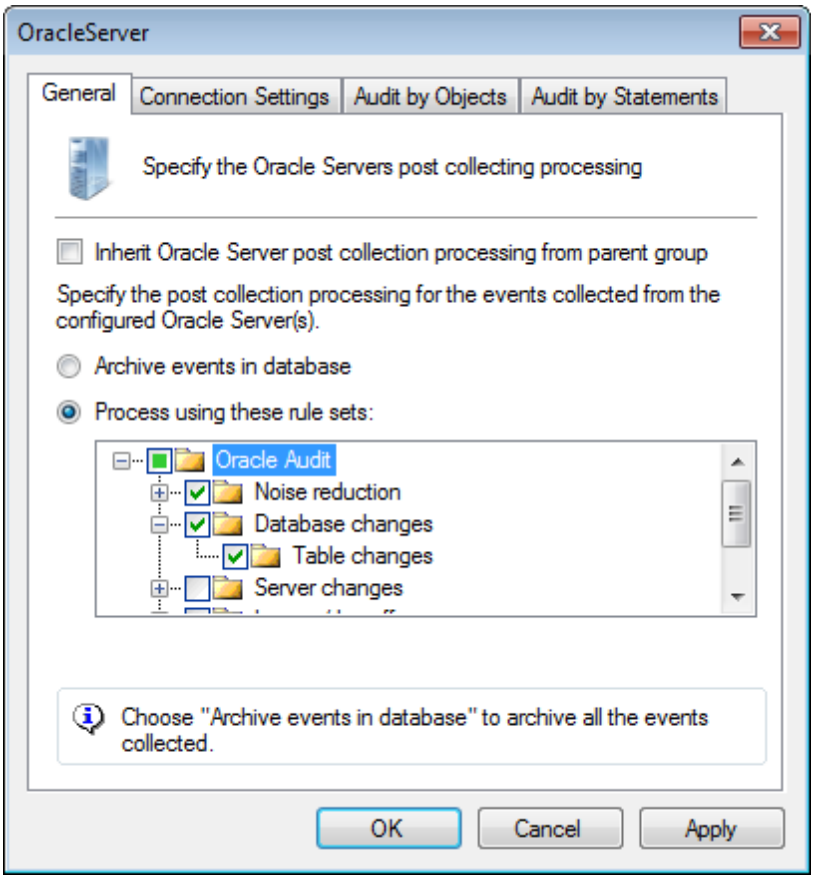
Captura de pantalla 64: Agregar nuevo servidor Oracle

2. Escriba el nombre del servidor o la dirección IP y haga clic en **Add**.

3. Haga clic en **Finish**; se cierra el cuadro de diálogo Add New Oracle Servers.

Nota

Use **Select** e **Import** para buscar en la red SQL Server® o importar la lista de SQL Server® desde un archivo de texto, respectivamente.

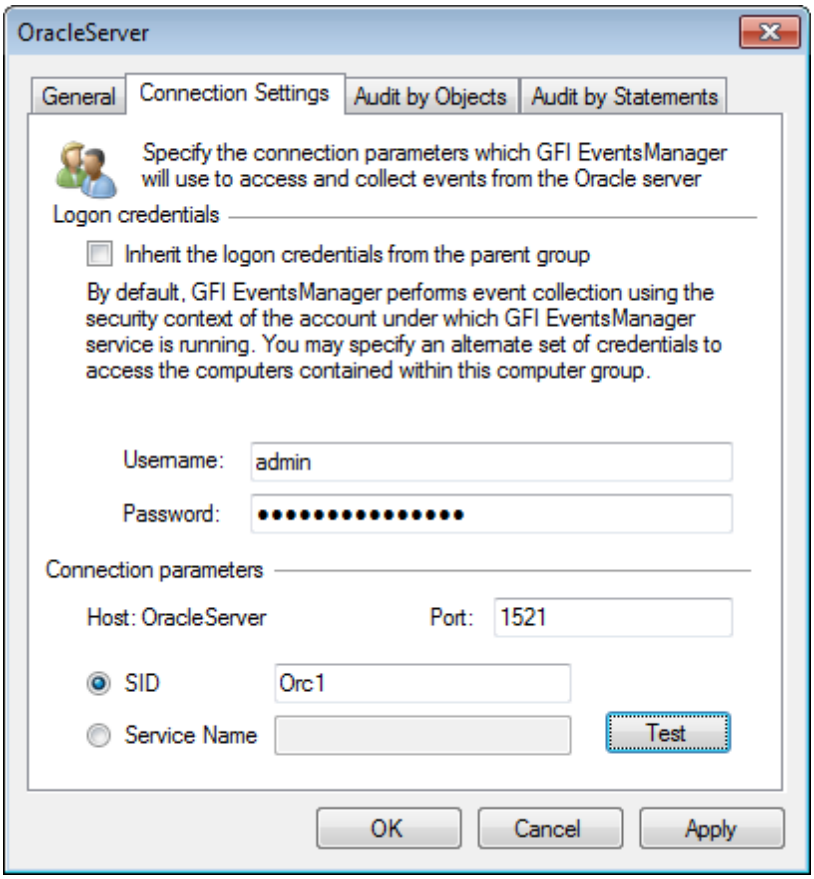


Captura de pantalla 65: Ficha Oracle Server properties - General

4. En el panel derecho, haga doble clic en el nuevo origen de eventos del servidor Oracle y configure las opciones que se describen a continuación:

Tabla 32: Ficha Oracle Server properties - General

Opción	Description
Inherit Oracle Server post collecting processing from parent group	Seleccione esta opción para heredar toda la configuración del grupo primario.
Archive events in database	Permite archivar eventos en el back-end de la base de datos de GFI EventsManager sin aplicar reglas de procesamiento.
Process using these rule sets	Permite especificar las reglas que desea ejecutar antes de archivar eventos en el back-end de la base de datos de GFI EventsManager.

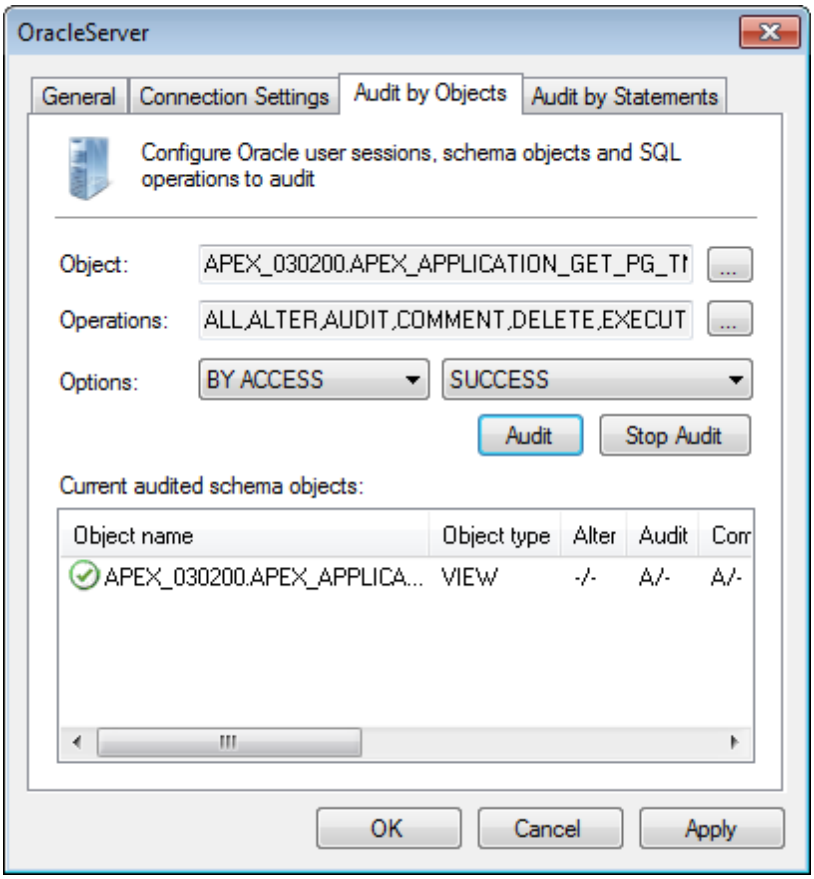

OracleServer
General
Connection Settings
Audit by Objects
Audit by Statements
Specify the connection parameters which GFI EventsManager will use to access and collect events from the Oracle server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Username:
admin
Password:
Connection parameters
Host: OracleServer
Port:
1521
SID
Orc1
Service Name
Test
OK
Cancel
Apply

Captura de pantalla 66: Ficha Oracle Server properties - Connection Settings

5. Seleccione **Connection Settings** y configure las opciones que se describen a continuación:

Tabla 33: Ficha Oracle Server properties - Connection Settings

Opción	Description
Inherit the logon credentials from the parent group	Seleccione esta opción para heredar la configuración de inicio de sesión del grupo primario.
Port	Ingrese el puerto que se utilizará para conectarse a la base de datos de Oracle.
SID	El SID es un nombre único para identificar una instancia de base de datos de Oracle. Ingrese el SID de la base de datos a auditar.
Service Name	El nombre de servicio es el alias utilizado para identificar la base de datos de Oracle. Ingrese el nombre de servicio de la base de datos a auditar.
Test	Pruebe la conexión con el servidor de la base de datos de Oracle.

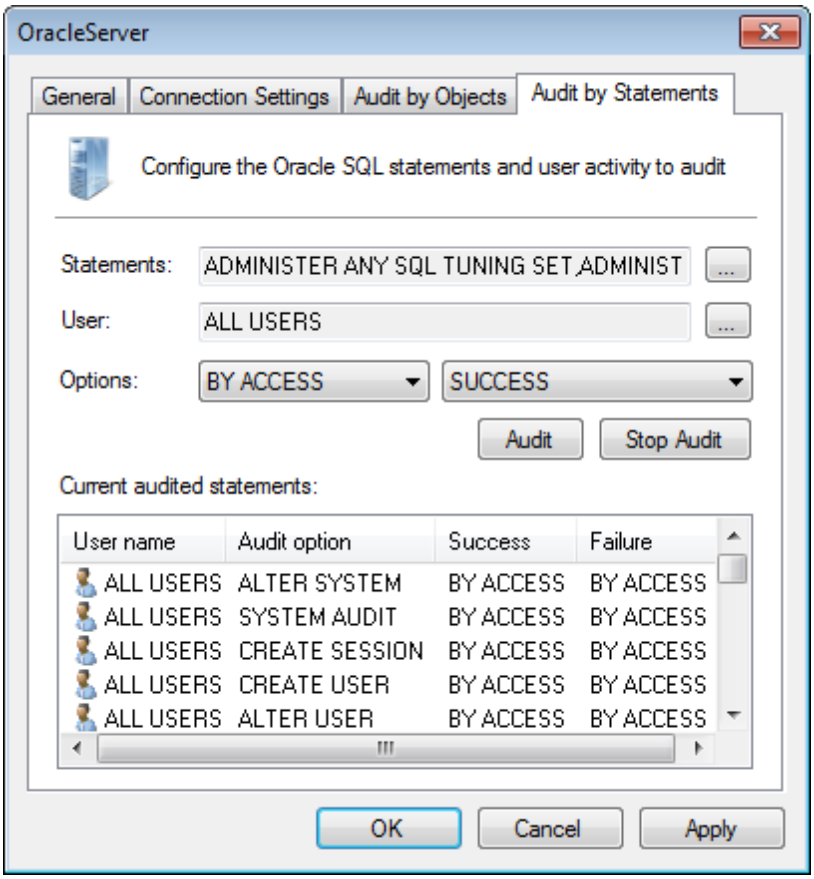


Captura de pantalla 67: Ficha Oracle Server properties - Audit by Objects

6. Seleccione **Audit by Objects** y configure las opciones que se describen a continuación:

Tabla 34: Ficha Oracle Server properties - Audit by Objects

Opción	Description
Object	Haga clic en **Browse** para abrir una lista de los objetos de Oracle disponibles. Seleccione el objeto a auditar y haga clic en **OK**. **NOTA**: Entre otras cosas, los objetos de Oracle pueden ser procedimientos, vistas, funciones y tablas.
Operations	Las operaciones son acciones que modifican o consultan un objeto. Haga clic en **Browse** para abrir una lista de operaciones disponibles. Seleccione las operaciones a auditar y haga clic en **OK**.
Opciones	Seleccione las opciones de auditoría: » **By Access**: crea un registro de auditoría por cada ejecución de operación de un objeto. » **By Session**: crea un registro de auditoría por cada operación y por cada objeto de esquema. Una sesión es el tiempo entre una conexión y una desconexión de la base de datos. » **Success**: seleccione esta opción para procesar solamente auditorías exitosas. » **Failure**: seleccione esta opción para procesar solamente las auditorías fallidas. Oracle crea un registro de auditoría si la auditoría no se completa. » **Both**: seleccione esta opción para procesar todos los registros de auditoría.
Audit	Elija esta opción para indicarle al servidor de Oracle que inicie la auditoría de las actividades del servidor correspondientes a los parámetros seleccionados (como usuarios, declaraciones, etc.)
Stop Audit	Seleccione esta opción para indicarle al servidor de Oracle que detenga la auditoría de las actividades del servidor correspondientes a los parámetros seleccionados (como usuarios, declaraciones, etc).
Current audited schema objects	Una lista que muestra todos los esquemas actuales de Oracle auditados.



Captura de pantalla 68: Ficha Oracle Server properties - Audit by Statements

7. Seleccione **Audit by Statements** y configure las opciones que se describen a continuación:

Tabla 35: Ficha Oracle Server properties - Audit by Statements

Opción	Description
Statements	Haga clic en **Browse** para abrir una lista de declaraciones de Oracle disponibles. Seleccione las declaraciones de Oracle para auditar y haga clic en **OK**. **NOTA**: Entre otras, las declaraciones de Oracle pueden ser **ALTER**, **CREATE** y **SELECT**.
User	Oracle le permite auditar las declaraciones de un usuario específico. Haga clic en el botón **Browse** para abrir una lista de usuarios disponibles. Seleccione el usuario y haga clic en **OK**.
Opciones	Seleccione las opciones de auditoría: » **By Access**: crea un registro de auditoría para cada ejecución de la declaración. » **By Session**: crea un registro de auditoría por usuario y por objeto de esquema. Una sesión es el tiempo entre una conexión y una desconexión de la base de datos. » **Success**: procesa solamente las auditorías exitosas. » **Failure**: seleccione la opción para procesar solamente las auditorías fallidas. Oracle crea un registro de auditoría si la auditoría no se completa. » **Both**: seleccione la opción para procesar todos los registros de auditoría.
Audit	Elija esta opción para indicarle al servidor de Oracle que inicie la auditoría de las actividades del servidor correspondientes a los parámetros seleccionados (como usuarios, declaraciones, etc.)
Stop Audit	Seleccione esta opción para indicarle al servidor de Oracle que detenga la auditoría de las actividades del servidor correspondientes a los parámetros seleccionados (como usuarios, declaraciones, etc).
Current audited statements	Una lista que muestra todas las declaraciones auditadas de Oracle actuales.

8. Haga clic en **Apply** y **OK**.

5 Recopilar registros de eventos

En este capítulo, se proporciona información acerca de cómo configurar los orígenes de eventos para aplicar reglas de procesamiento de eventos a los eventos recopilados. Asigne reglas de procesamiento de eventos existentes o personalizados para procesar con precisión solamente los eventos deseados.

Temas de este capítulo:

5.1 Recopilar registros de eventos de Windows® 103

5.2 Recopilar registros de texto 106

5.3 Recopilar Syslogs 109

5.4 Recopilar mensajes de capturas SNMP 113

5.5 Recopilar registros personalizados 117

5.6 Recopilar registros de eventos de GFI LanGuard 119

5.7 Recopilar eventos de GFI EndPointSecurity 124

5.1 Recopilar registros de eventos de Windows®

Los eventos de Windows® se organizan en categorías de registros específicos. De forma predeterminada, los equipos que se ejecutan en Windows® NT o en una versión superior de Windows registran errores, advertencias y eventos de información en tres registros. Concretamente, estos son registros de **Seguridad**, **Aplicaciones** y **Registros del sistema**.

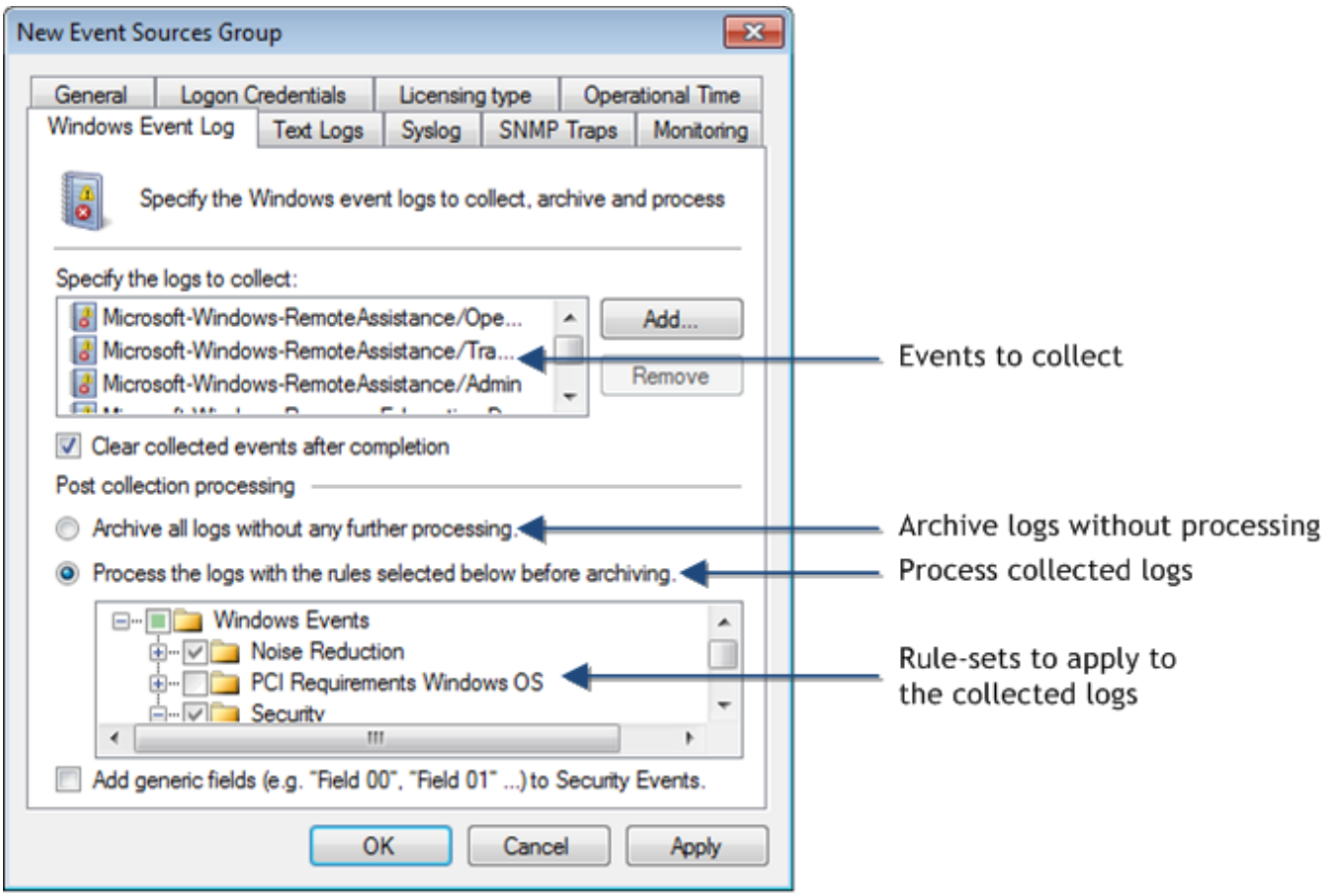
Los equipos que tienen funciones más especiales en la red, como los controladores de dominio y los servidores DNS, tienen categorías de registro de eventos adicionales.

Como mínimo, los sistemas operativos Windows® registran eventos en los siguientes registros:

Tabla 36: Registro de eventos de Windows® recopilados por GFI EventsManager

Tipo de registro	Descripción
Registro de eventos de seguridad	Este registro contiene eventos relacionados con la seguridad a través de los cuales puede auditar los intentos de infracción de seguridad o las infracciones de seguridad exitosas. Eventos típicos que se encuentran en el registro de eventos de seguridad incluyen intentos de inicio de sesión válidos y no válidos.
Registro de eventos de aplicaciones	Este registro contiene eventos registrados por las aplicaciones de software, como los errores de archivos.
Registro de eventos del sistema	Este registro contiene eventos registrados por los componentes del sistema operativo, como los errores al cargar controladores de dispositivos.
Registro de servicio de directorio	Este registro contiene los eventos generados por Active Directory, entre los que se incluyen los intentos exitosos o fallidos de actualizar la base de datos de Active Directory.
Registro de servicio de replicación de archivos	Este registro contiene eventos registrados por el servicio de replicación de archivos de Windows®. Estos incluyen los errores y eventos de replicación de archivos que ocurren mientras se actualizan los controladores de dominio con información sobre SYSVOL.
Registro del servidor DNS	Este registro contiene los eventos asociados con el proceso de resolución de nombres DNS en direcciones IP.

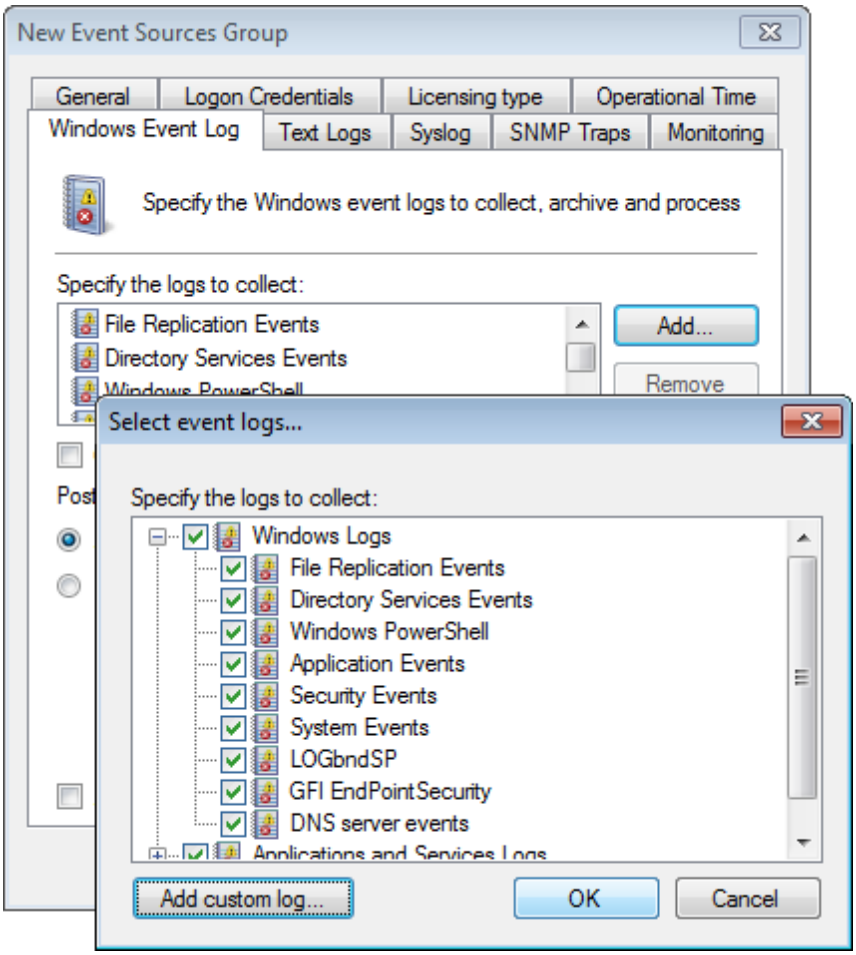
Tipo de registro	Descripción
Registros de aplicaciones y servicios	Estos registros contienen eventos asociados con Windows® Vista, y los servicios y las funciones relacionadas que este ofrece.



Captura de pantalla 69: Propiedades del grupo de equipos: Configurar parámetros de registros de eventos de Windows®

Para configurar parámetros de recopilación y procesamiento de registros de eventos de Windows®:

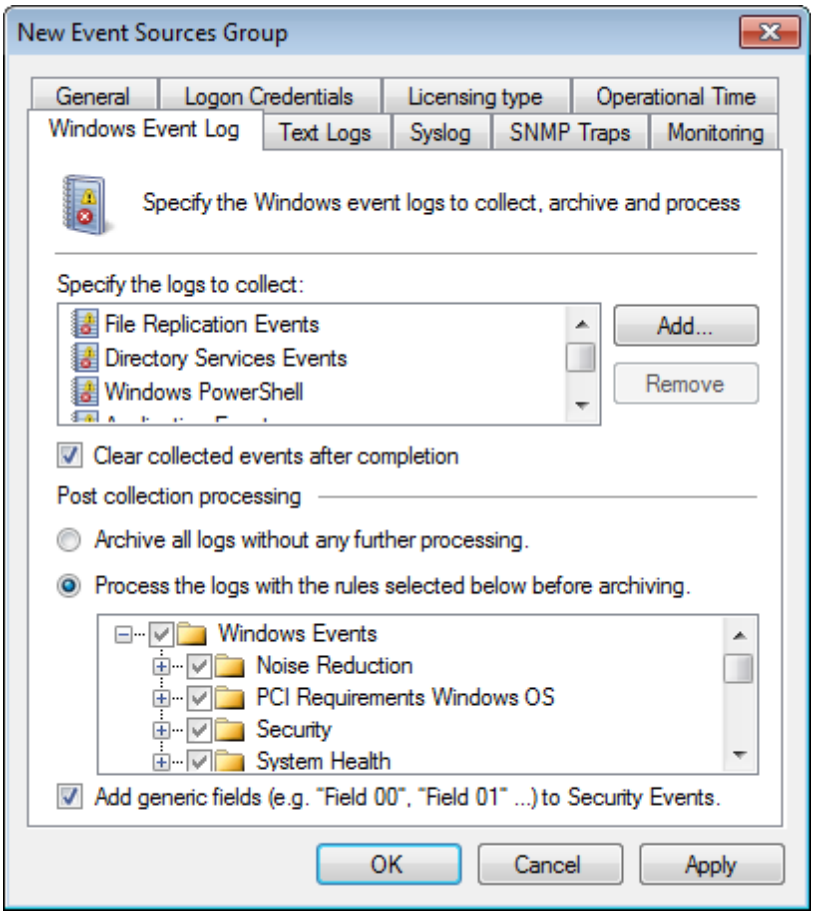
1. En la ficha **Configuration > Event Sources**, haga clic con el botón secundario en un origen de eventos y seleccione **Properties**.



Captura de pantalla 70: Seleccionar registros de eventos que desea recopilar

2. Haga clic en la ficha **Windows Event Log > Add...** para seleccionar los registros que desea recopilar. Expanda **Windows Logs** o **Applications and Services Logs** y seleccione una opción de la lista de registros disponibles.

3. (Opcional) Haga clic en **Add custom log...** e ingrese un nombre único para el registro de eventos que no figure en la lista.



Captura de pantalla 71: Configurar parámetros de procesamiento del registro de eventos de Windows

4. Seleccione **Clear collected events after completion** para borrar los eventos recopilados desde el origen del evento en cuestión.

5. Seleccione **Archive events in database** para archivar los eventos recopilados sin aplicar las reglas de procesamiento de eventos.

6. Seleccione **Process using these rule sets** y seleccione los conjuntos de reglas que desee ejecutar contra los eventos recopilados.

7. Seleccione **Add generic fields** para agregar campos extendidos a la base de datos. Los campos extendidos contienen datos de descripciones de eventos y se agregan por un nombre común (por ejemplo: "Campo01","Nombre de campo personalizado").

8. Haga clic en **Apply** y **OK**.

Importante

Eliminar registros de eventos sin archivar puede dar lugar a penalizaciones legales.

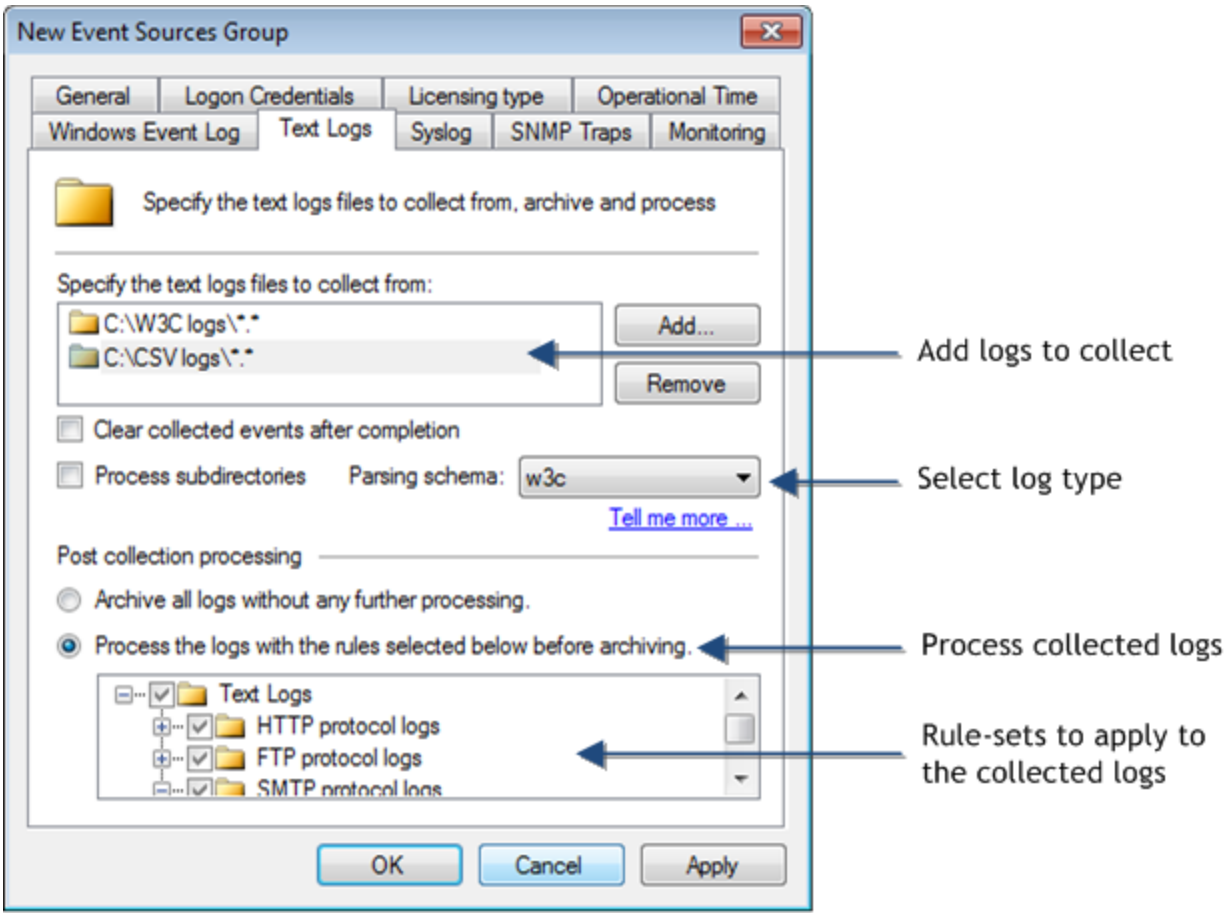
5.2 Recopilar registros de texto

Los registros de texto son otros formatos de registro compatibles con GFI EventsManager. Los registros W3C son archivos planos basados en texto que contienen diversos detalles de eventos delimitados por caracteres especiales.

Comúnmente, los sistemas de hardware (por ejemplo: servidores y dispositivos) que tienen roles específicos de Internet usan el formato de registro W3C. Microsoft® Por ejemplo, el servicio Internet

Information Server (IIS) y los servidores web Apache pueden recopilar eventos relacionados con la web, como registros web en forma de archivos de texto con formato W3C.

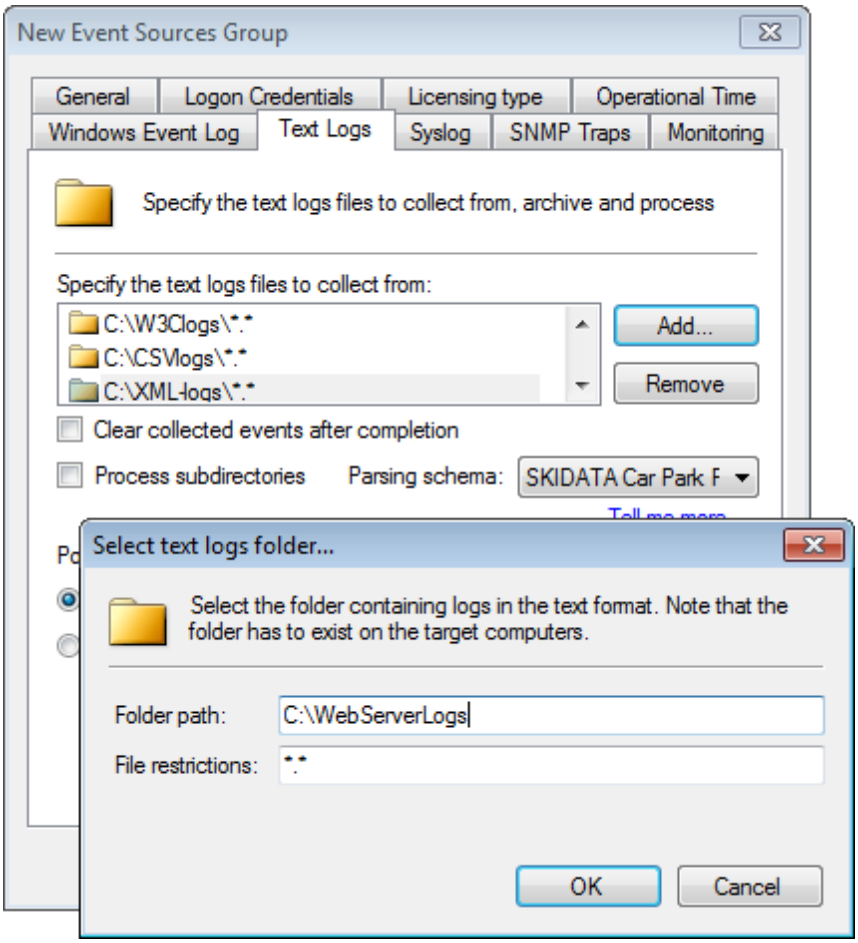
En GFI EventsManager, el proceso de configuración de los parámetros de registro W3C es idéntico al que se realiza para el procesamiento de eventos de Windows®, con una excepción. A diferencia de los registros de eventos de Windows®, no hay ninguna norma que dicte una ubicación de carpeta específica o centralizada donde los archivos de registro W3C se almacenen en el disco. Por lo tanto, para recopilar los registros W3C, debe especificar la ruta de acceso completa a estos archivos de registro basados en texto.



Captura de pantalla 72: Opciones de registros de texto

Para recopilar registros de texto:

1. En la ficha **Configuration > Event Sources**, haga clic con el botón secundario en un origen de eventos y seleccione **Properties**.



Captura de pantalla 73: Agregar carpetas que contienen registros de texto

2. Haga clic en la ficha **Text Logs > Add...** para agregar las rutas de las carpetas que contengan registros de texto.

3. En el cuadro de diálogo **Select text logs folder...**, escriba la ruta a la carpeta que contenga los archivos de registros de texto y haga clic en **OK**.

4. Seleccione **Clear collected events after completion** para borrar los eventos recopilados desde el origen del evento en cuestión.

5. Seleccione **Process subdirectories** para analizar de forma recursiva la ruta especificada que contenga los registros de texto.

6. En el menú desplegable **Parsing schema**, seleccione el esquema en el que se interpretan los registros de texto. Seleccione una de las siguientes opciones:

- W3C
- CSV
- DHCP
- XML
- Registros SAP
- Registros ESM
- Pagos estacionamiento de vehículos SKI Data

7. Seleccione **Archive events in database** para archivar los eventos recopilados sin aplicar las reglas de procesamiento de eventos.

8. Seleccione **Process using these rule sets** y seleccione los conjuntos de reglas que desee ejecutar contra los eventos recopilados.

9. Haga clic en **Aplicar** y **Aceptar**.

Importante

Eliminar registros de eventos sin archivar puede dar lugar a penalizaciones legales.

5.3 Recopilar Syslogs

Syslog es un servicio de registro de datos que se usa más comúnmente en sistemas basados en Linux y UNIX. Syslogs se basa en el concepto de que un servidor dedicado llamado “Servidor Syslog” controla totalmente el registro de eventos e información.

A diferencia de Windows® y los sistemas basados en registros de texto, los dispositivos habilitados para Syslog envían eventos en forma de mensajes de datos (conocidos técnicamente como "Mensajes Syslog") a un servidor Syslog que interpreta y administra mensajes, y guarda los datos en un archivo de registro.

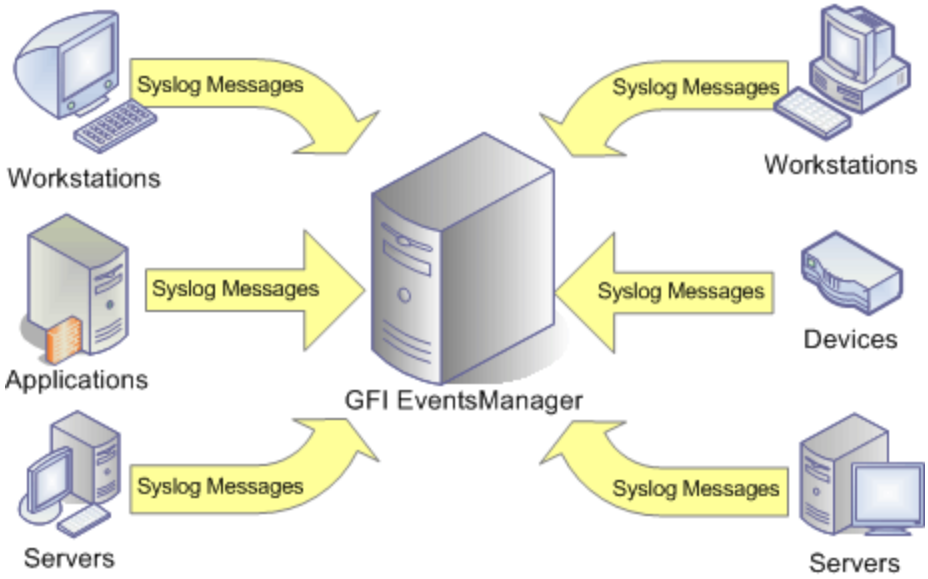
A fin de procesar los mensajes Syslog, GFI EventsManager se envía con un servidor Syslog integrado. Este servidor Syslog recopila de forma automática, en tiempo real, todos los mensajes y eventos Syslog enviados por los orígenes Syslog y los transfiere al motor de procesamiento de eventos. Listo para usar, GFI EventsManager es compatible con los eventos generados por los diversos dispositivos de red fabricados por proveedores líderes, como Cisco y Juniper.

Nota

Para obtener más información acerca de los dispositivos compatibles, visite el siguiente artículo de la base de conocimiento: http://go.gfi.com/?pageid=esm_syslog_snmp_support.

Nota

Un búfer incorporado permite que el servidor Syslog recopile, ponga en cola y reenvíe hasta 30 mensajes Syslog a la vez. De forma predeterminada, los registros almacenados en búfer pasan al motor de procesamiento de eventos no bien el búfer se llena o a intervalos de un minuto, lo que ocurra primero.



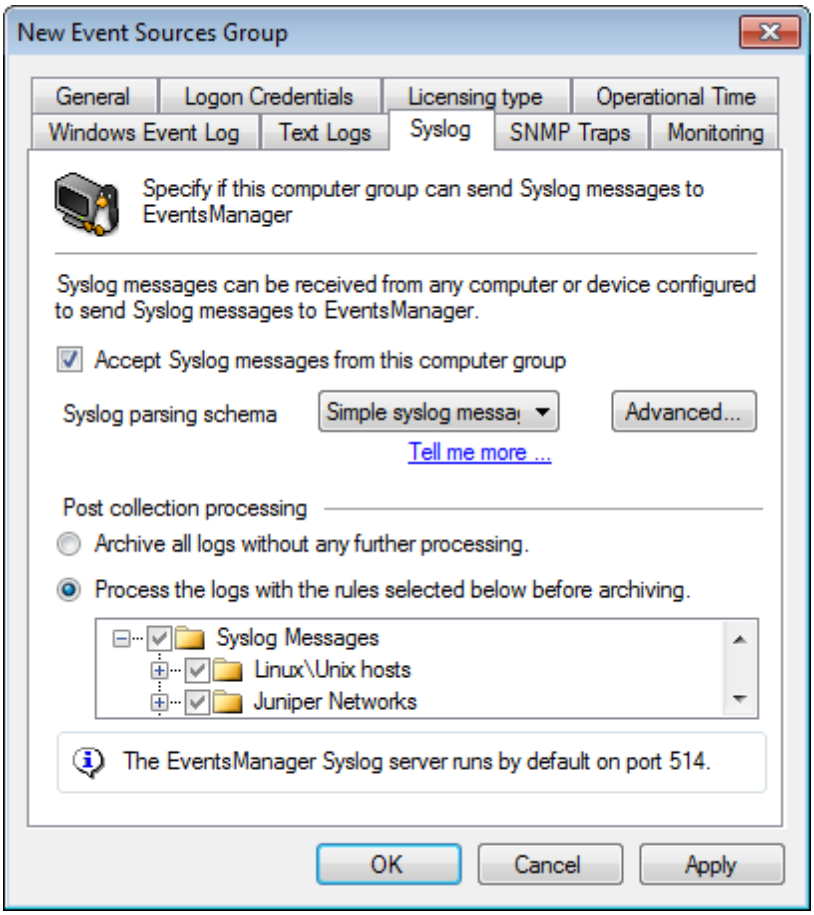
Captura de pantalla 74: Se deben dirigir los mensajes Syslog al equipo que ejecuta GFI EventsManager.

Importante

Antes de empezar a recopilar Syslogs, se debe configurar cada origen de eventos Syslog (estaciones de trabajo, servidores o dispositivos de red) para enviar sus mensajes Syslog al nombre o la dirección IP del equipo donde está instalado GFI EventsManager.

Para recopilar Syslogs:

1. En la ficha **Configuration > Event Sources**, haga clic con el botón secundario en un origen de eventos y seleccione **Properties**.



Captura de pantalla 75: Recopilar Syslogs - Opciones de Syslogs

2. Haga clic en la ficha **Syslog** y seleccione **Accept Syslog messages to EventsManager** para permitir la recopilación de Syslogs de ese origen de eventos o grupo de orígenes de eventos.

3. En el menú desplegable **Syslog parsing schema**, seleccione el método con que el servidor Syslog de GFI EventsManager interpreta los mensajes Syslog de los dispositivos de red. Seleccione una de las siguientes opciones:

- Mensaje Syslog simple
- Mensaje estándar de Linux
- Firewall de red Juniper
- Cisco ASA

4. Haga clic en **Advanced…** para usar la página de códigos de Windows personalizada. Especifique el código y haga clic **OK**.

Nota

La página de códigos de Windows® se usa para codificar caracteres internacionales en cadenas ASCII. Puesto que Syslog no es compatible con Unicode, GFI EventsManager usa una página de códigos para decodificar los eventos. Esto solamente es aplicable si GFI EventsManager se instaló en una máquina que usa un lenguaje distinto al de los equipos supervisados. Para obtener más información, consulte http://go.gfi.com/?pageid=esm_code_page.

5. Seleccione **Archive events in database** para archivar los eventos recopilados sin aplicar las reglas de procesamiento de eventos.

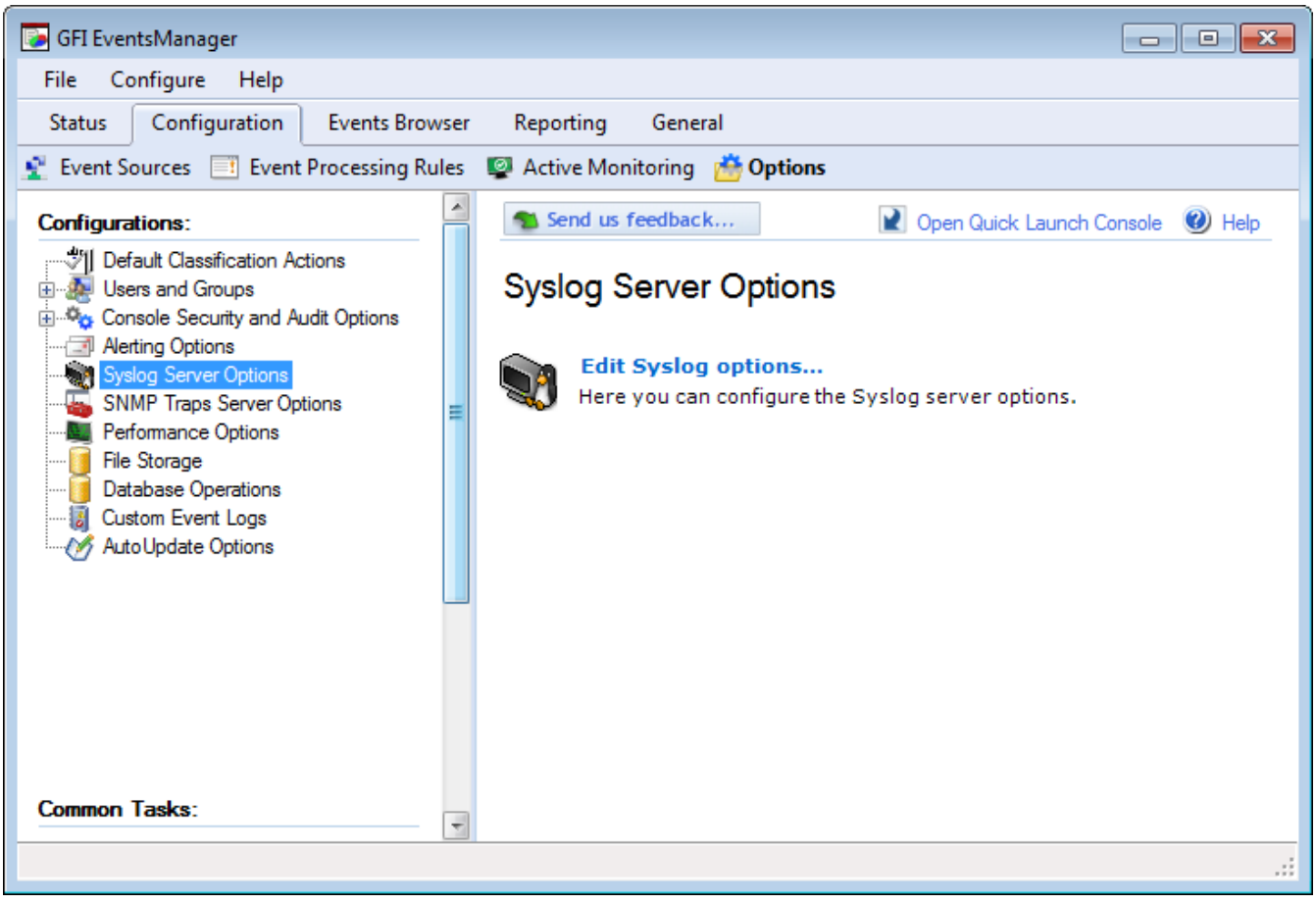
6. Seleccione **Process using these rule sets** y seleccione los conjuntos de reglas que desee ejecutar contra los eventos recopilados.

7. Haga clic en **Apply** y **OK**.

> **Nota**
>
> El servidor Syslog de GFI EventsManager está configurado de forma predeterminada para recibir los mensajes Syslog en el puerto **514**. Para obtener más información, consulte Configurar puerto de comunicaciones del servidor Syslog.

> **Importante**
>
> Eliminar registros de eventos sin archivar puede dar lugar a penalizaciones legales.

5.3.1 Configurar puerto de comunicaciones del servidor Syslog

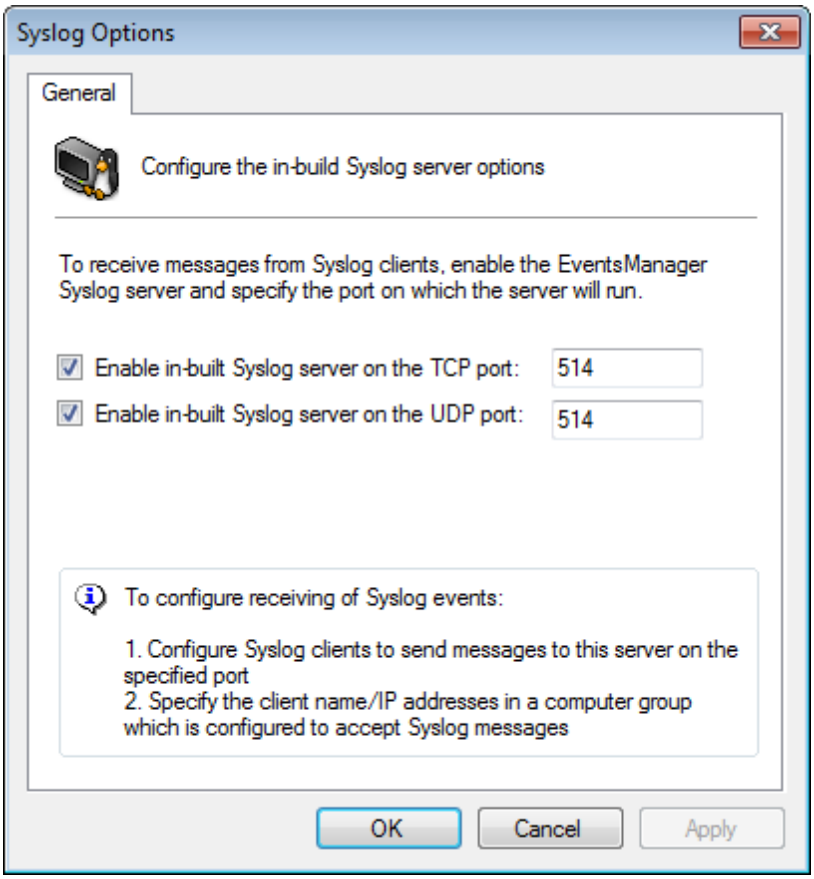


Captura de pantalla 76: Configurar puerto de comunicaciones del servidor Syslog

Para cambiar la configuración predeterminada de los puertos Syslog:

1. Haga clic en la ficha **Configuration** > **Options**.

2. Haga clic con el botón secundario en **Syslog Server Options** y seleccione **Edit Syslog options...**.


Syslog Options
General
Configure the in-build Syslog server options
To receive messages from Syslog clients, enable the EventsManager Syslog server and specify the port on which the server will run.
Enable in-built Syslog server on the TCP port:
514
Enable in-built Syslog server on the UDP port:
514
To configure receiving of Syslog events:
1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages
OK
Cancel
Apply

Captura de pantalla 77: Opciones de servidor Syslog

4. Seleccione **Enable in-built Syslog server on TCP port:** y especifique el puerto TCP en el que GFI EventsManager recibirá los mensajes Syslog.

5. Seleccione **Enable in-built Syslog server on UDP port:** y especifique el puerto UDP en el que GFI EventsManager recibirá los mensajes Syslog.

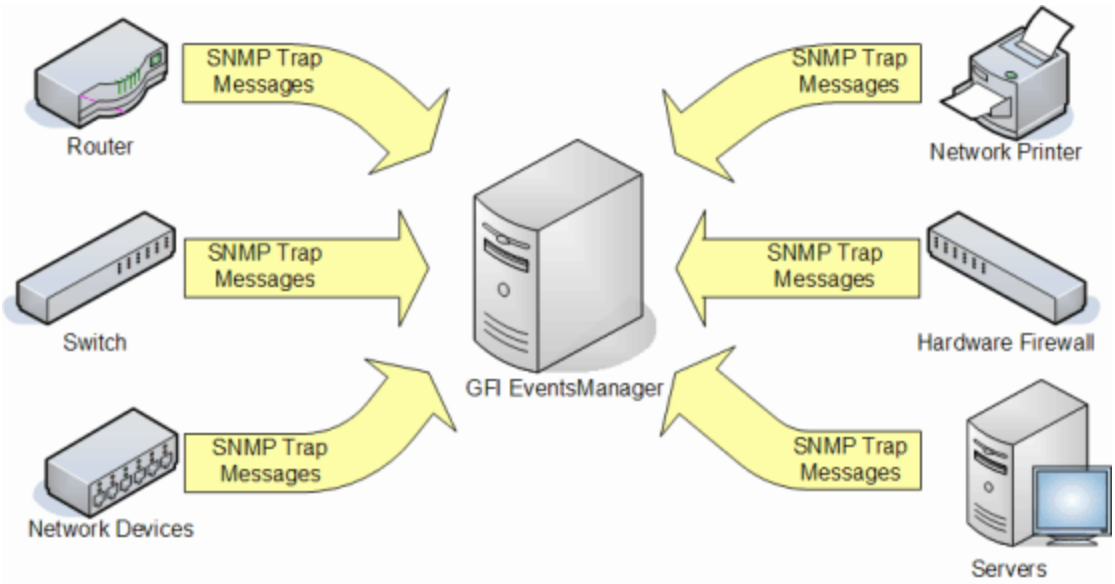
6. Haga clic en **Apply** y **OK**.

Nota

Cuando configure los parámetros del puerto del servidor Syslog, asegúrese de que el puerto configurado no esté ya en uso por otras aplicaciones instaladas. Ello puede afectar la entrega de mensajes Syslog a GFI EventsManager.

5.4 Recopilar mensajes de capturas SNMP

SNMP es un servicio de registro de datos que permite que los dispositivos conectados en red puedan registrar eventos e información por medio de mensajes de datos (conocidos técnicamente como capturas SNMP). La tecnología de mensajería SNMP es similar en concepto a Syslogs, donde, a diferencia deWindows® y de los entornos basados en registros de eventos, los dispositivos que generan mensajes SNMP no registran datos de eventos en los registros locales. En cambio, la información de los eventos se envía en forma de mensajes de datos a un servidor de captura SNMP que administra y guarda los datos de mensajes SNMP en un archivo de registro local (centralizado).



Captura de pantalla 78: Se deben dirigir los mensajes de captura SNMP al equipo que ejecuta GFI EventsManager.

Nota

GFI EventsManager es compatible de forma nativa con una amplia lista de dispositivos SNMP y bases de información de administración (MIB, por sus siglas en inglés). Para obtener una lista completa de los dispositivos compatibles, consulte el siguiente artículo de la base de conocimiento: http://go.gfi.com/?pageid=esm_syslog_snmp_support.

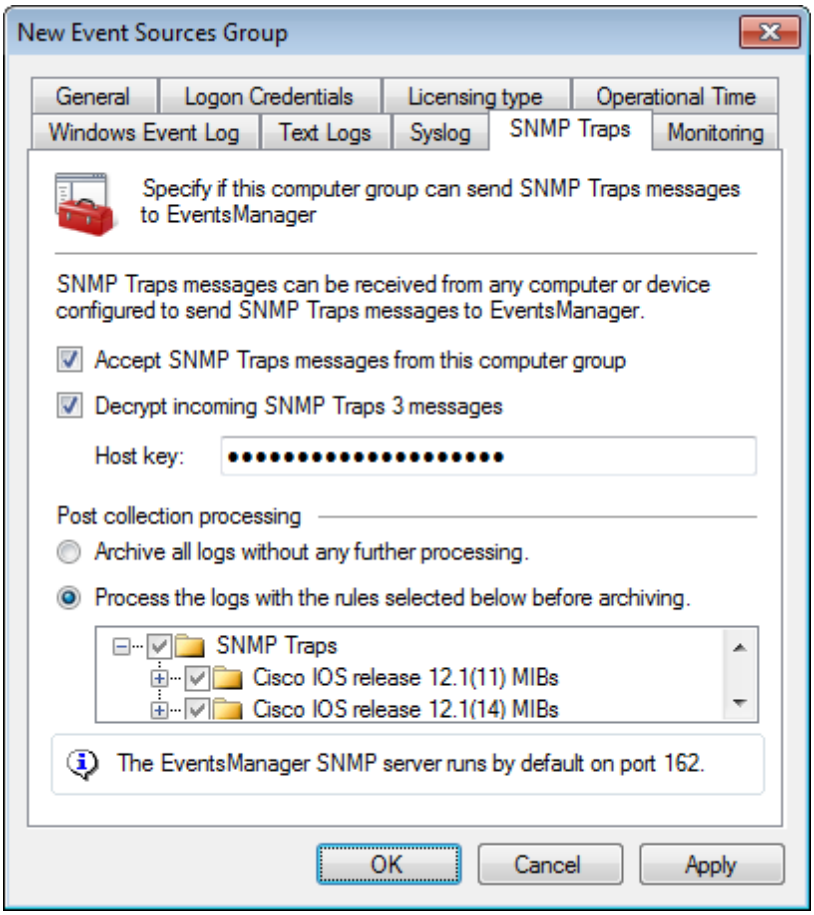
GFI EventsManager incluye un servidor de captura SNMP dedicado a través del cual se administran las capturas SNMP. Un búfer integrado permite al servidor de captura SNMP recopilar, poner en cola y reenviar hasta 30 capturas SNMP a la vez. De forma predeterminada, los registros almacenados en búfer pasan al motor de procesamiento de eventos no bien el búfer se llena o a intervalos de un minuto, lo que ocurra primero.

Importante

Antes de empezar a recopilar los mensajes de captura SNMP, cada origen de evento SNMP (estaciones de trabajo, servidores o dispositivos de red) debe estar configurado para enviar sus mensajes de captura SNMP al nombre o la dirección IP del equipo donde está instalado GFI EventsManager.

Para recopilar capturas SNMP:

1. En la ficha **Configuration > Event Sources**, haga clic con el botón secundario en un origen de eventos y seleccione **Properties**.


New Event Sources Group
General
Logon Credentials
Licensing type
Operational Time
Windows Event Log
Text Logs
Syslog
SNMP Traps
Monitoring
Specify if this computer group can send SNMP Traps messages to EventsManager
SNMP Traps messages can be received from any computer or device configured to send SNMP Traps messages to EventsManager.
Accept SNMP Traps messages from this computer group
Decrypt incoming SNMP Traps 3 messages
Host key:
Post collection processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
SNMP Traps
Cisco IOS release 12.1(11) MIBs
Cisco IOS release 12.1(14) MIBs
The EventsManager SNMP server runs by default on port 162.
OK
Cancel
Apply

Captura de pantalla 79: Recopilar capturas SNMP

2. Haga clic en la ficha **SNMP Traps** y seleccione **Accept SNMP Traps messages from this event source** para activar la recopilación de capturas SNMP.

3. Seleccione **Decrypt incoming SNMP Traps 3 messages** y especifique la clave de seguridad en el cuadro de texto **Host key**.

4. Seleccione **Archive events in database** para archivar los eventos recopilados sin aplicar las reglas de procesamiento de eventos.

5. Seleccione **Process using these rule sets** y seleccione los conjuntos de reglas que desee ejecutar contra los eventos recopilados.

6. Haga clic en **Apply** y **OK**.

Nota

El servidor de captura SNMP de GFI EventsManager está configurado de forma predeterminada para escuchar los mensajes de captura SNMP en el puerto **162**. Para obtener más información, consulte Configurar servidor de capturas SNMP.

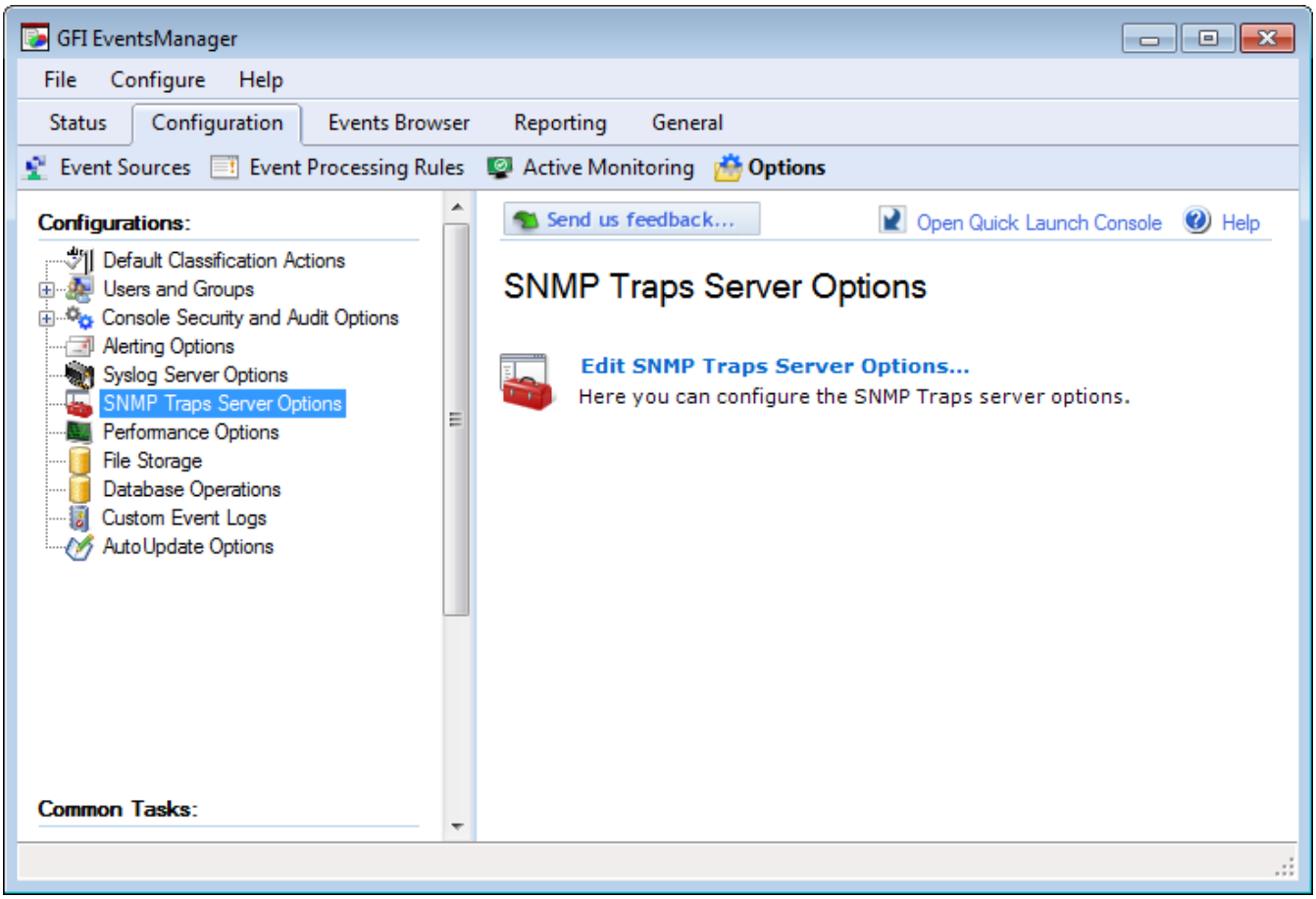
Nota

El servidor de captura SNMP integrado es compatible con las capturas cifradas de la versión 3 de SNMP. Para los mensajes SNMP cifrados, la clave de host de cifrado se debe especificar en el campo de descifrado de mensajes entrantes de capturas SNMP 3.

Importante

Eliminar registros de eventos sin archivar puede dar lugar a penalizaciones legales.

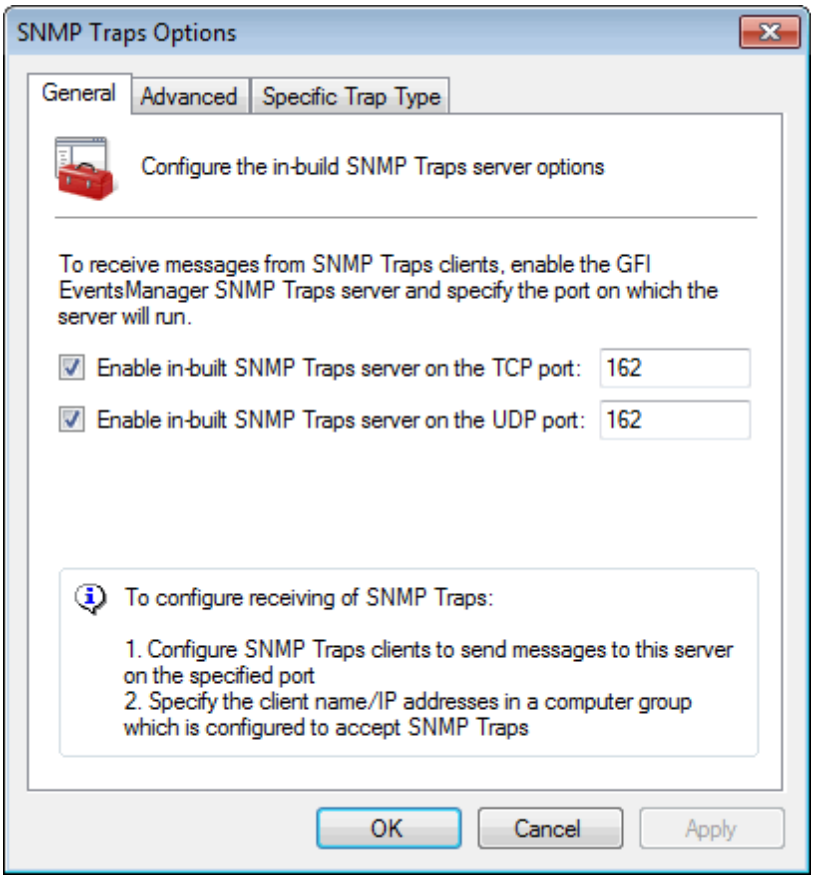
5.4.1 Configurar servidor de capturas SNMP



Captura de pantalla 80: Configurar capturas SNMP

Para cambiar la configuración predeterminada del servidor de capturas SNMP:

1. Haga clic en la ficha **Configuration** > **Options**.
2. Haga clic con el botón secundario en **SNMP Traps Options** y seleccione **Edit SNMP Traps options…**.


SNMP Traps Options
General
Advanced
Specific Trap Type
Configure the in-build SNMP Traps server options
To receive messages from SNMP Traps clients, enable the GFI EventsManager SNMP Traps server and specify the port on which the server will run.
Enable in-built SNMP Traps server on the TCP port:
162
Enable in-built SNMP Traps server on the UDP port:
162
To configure receiving of SNMP Traps:
1. Configure SNMP Traps clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept SNMP Traps
OK
Cancel
Apply

Captura de pantalla 81: Opciones de capturas SNMP

3. Habilite el servidor SNMP TCP/UDP requerido. Especifique el puerto TCP/UDP en el cual GFI EventsManager recibirá los mensajes SNMP.

4. Haga clic en la ficha **Advanced** para agregar, editar o eliminar los ID de objeto de captura (OID, por sus siglas en inglés) SNMP.

5. Haga clic en la ficha **Specific Trap Type** para agregar, editar o eliminar tipos de captura.

6. Haga clic en **Apply** y **OK**.

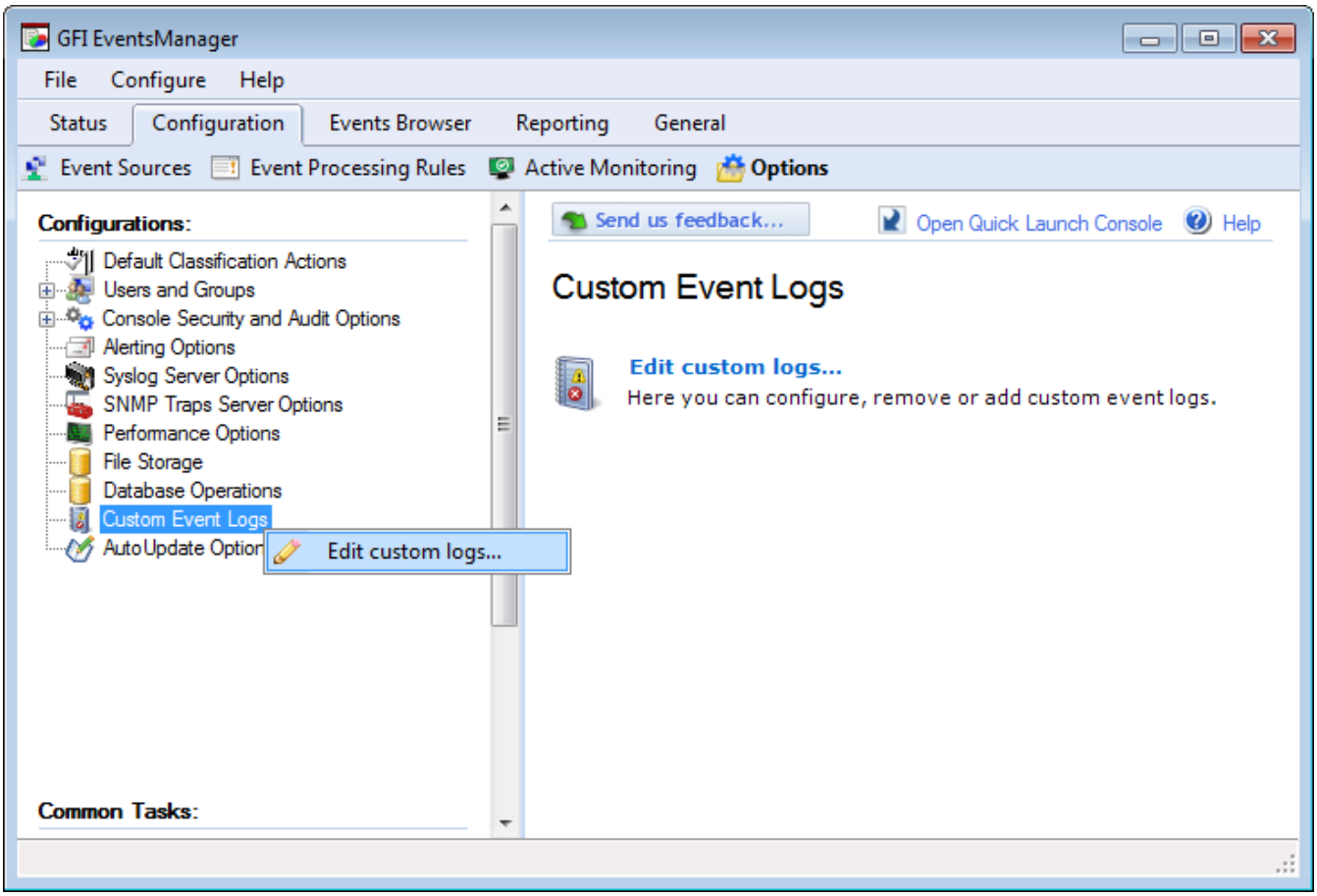
> **Nota**
>
> Al configurar los parámetros del puerto del servidor de captura SNMP, asegúrese de que el puerto TCP o UDP configurado no se esté ya en uso por otras aplicaciones instaladas. Ello puede afectar la entrega de mensajes de captura SNMP a GFI EventsManager.

5.5 Recopilar registros personalizados

GFI EventsManager está configurado para recopilar y procesar registros de eventos estándar. Sin embargo, también se puede configurar GFI EventsManager para administrar eventos registrados en aplicaciones de terceros, como los registros de antivirus, registros de firewall y otras aplicaciones de seguridad.

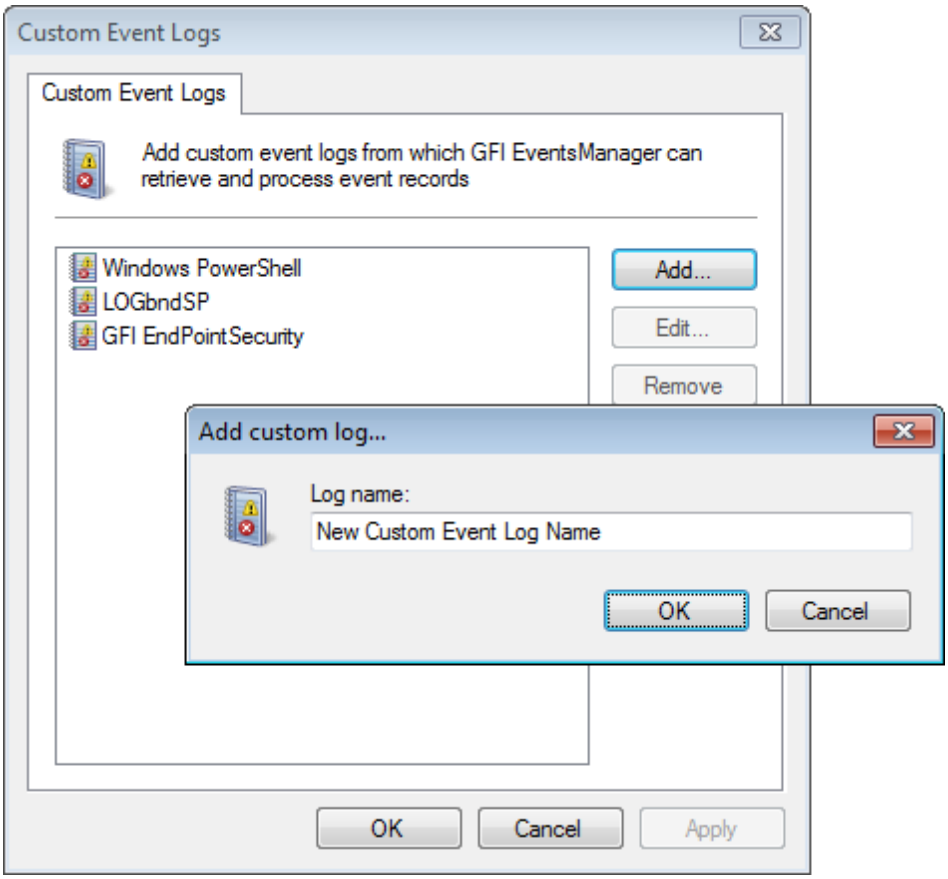
Para configurar eventos personalizados:

1. Haga clic en la ficha **Configuration** > **Options**.



Captura de pantalla 82: Configuración de registros de eventos personalizados

2. En **Configurations**, haga clic con el botón secundario en **Custom Event Logs** y seleccione **Edit custom logs…**.



Captura de pantalla 83: Cuadro de diálogo Custom event logs

3. Haga clic en el botón **Add…** y especifique el nombre de su registro de eventos personalizados.

4. Haga clic en **Aceptar**.

5. (Opcional) Haga clic en **Edit** para cambiar el nombre del evento personalizado seleccionado o haga clic en **Remove** para eliminar el evento personalizado seleccionado.

6. Haga clic en **Apply** y **OK**.

5.6 Recopilar registros de eventos de GFI LanGuard

GFI EventsManager le permite supervisar los eventos generados por GFI LanGuard. GFI LanGuard es una herramienta de análisis de vulnerabilidad de red que audita su red para detectar debilidades que podrían aprovechar usuarios con fines maliciosos. Durante las auditorías de red, GFI LanGuard crea eventos en el "**Application Log**" de la máquina en el que está instalado.

Por cada máquina que analiza GFI LanGuard, se genera una entrada "Aplication Log" con un "**Event ID: 0**" y con un "**Source**" definido como **GFI LanGuard**. Estos eventos denotan la información de vulnerabilidades de la red que se extrajo de los equipos analizados, incluso:

Tabla 37: Información recopilada por GFI LanGuard

Información recopilada	Descripción
Nivel de amenaza	Recopila información sobre el nivel general de amenazas en la red. Esta clasificación se genera a través de un extenso algoritmo después de que GFI LanGuard audita la red.
Revisiones y service packs faltantes	Averigüe a qué equipos le faltan actualizaciones y qué actualizaciones se deben instalar para reforzar el nivel de seguridad.
Puertos abiertos	Descubra todo puerto TCP o UDP abierto no deseado.

Información recopilada	Descripción
Estado de definición de funcionamiento de antivirus y malware	GFI LanGuard es capaz de verificar si las definiciones de su base de datos de virus están actualizadas. De no ser así, se le notificará y GFI LanGuard intentará actualizar las definiciones.
Aplicaciones que se detectaron en los objetivos analizados	GFI LanGuard enumera las aplicaciones que se instalaron en los objetivos analizados. Puede crear un inventario de las aplicaciones deseadas o no deseadas y configurar GFI LanGuard para que desinstale automáticamente las aplicaciones que se clasificaron como no deseadas.

Nota

Para obtener más información sobreGFI LanGuard, consulte http://www.gfi.com/network-security-vulnerability-scanner.

Nota

GFI EventsManager puede procesar los eventos generados por la versión 9.5 deGFI LanGuard o por una posterior.

5.6.1 Cómo habilitar el registro de eventos de GFI LanGuard

Hay dos pasos clave necesarios para habilitar la integración del registro de eventos entreGFI LanGuard y GFI EventsManager:

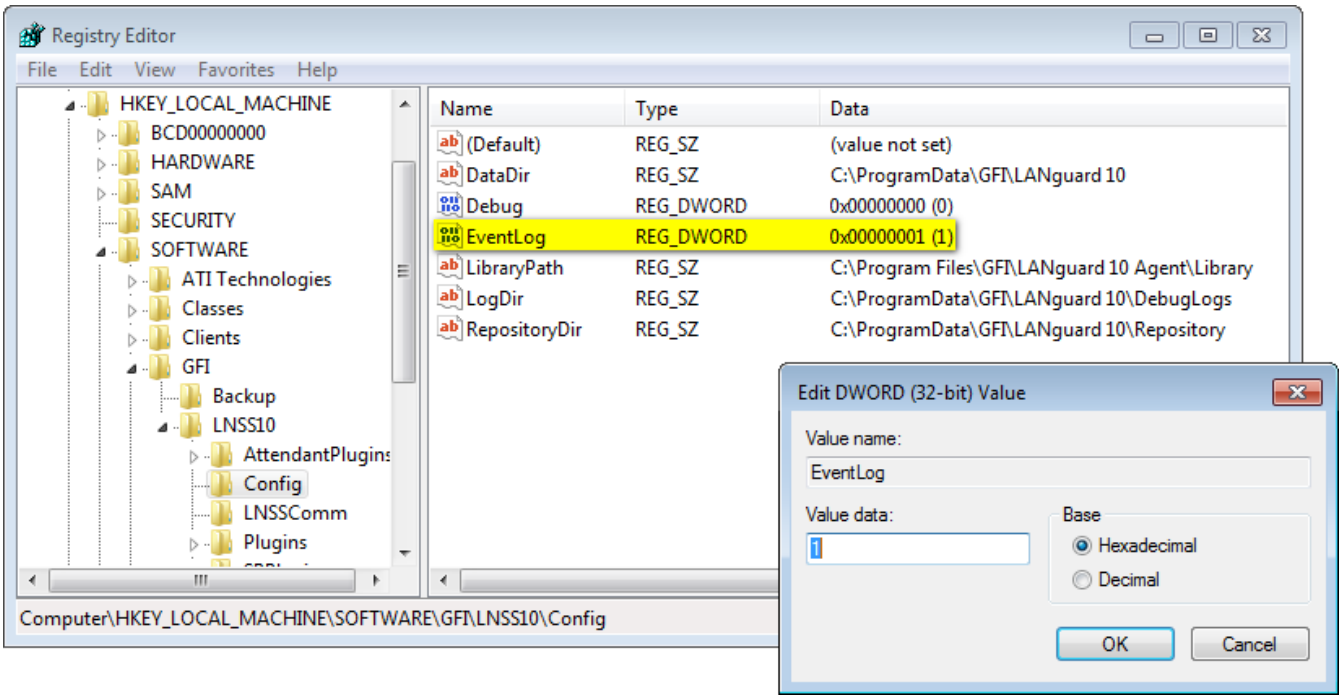
- Paso 1: Habilitar registro
- Paso 2: Configurar GFI EventsManager para que recopile registros de la aplicación

Paso 1: Habilitar registro de GFI LanGuard

Para permitir que GFI LanGuard genere registros de eventos una vez que finalizan las auditorías del sistema:

1. Agregue la máquina donde GFI LanGuard está instalado como un origen de eventos.

2. Haga clic en **Start > Run** y escriba **regedit**. Presione la tecla **Enter**.



Captura de pantalla 84: Habilitar el inicio de sesión de GFI LanGuard a través del registro de Windows

3. Vaya a la siguiente clave del registro y editar el valor para habilitar el registro de eventos:

» **Plataformas Windows® x86**:

- `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS[n]\Config`
- Defina el valor de **REG_DWORD EventLog** en **1**.

» **Plataformas Windows® x64**:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GFI\LNSS[n]\Config`
- Defina el valor de **REG_DWORD EventLog** en **1**.

Importante

[n] es el número de versión principal de GFI LanGuard.

Ejemplo: HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS**9**\Config\EventLog = 1(dword)

Nota

Para evitar que GFI LanGuard genere entradas "Application Log", elimine el valor de registro que se describió anteriormente o cambie el valor del registro a **0**.

Paso 2: Configurar GFI EventsManager para que recopile registros de aplicación

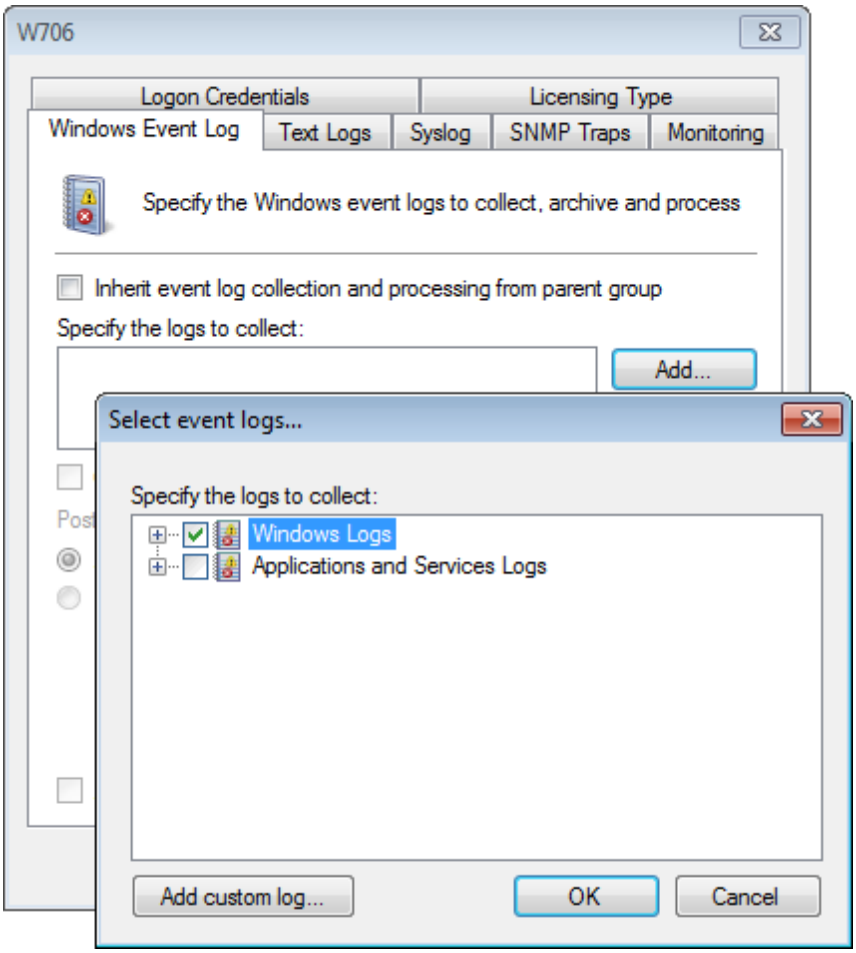
GFI LanGuard imprime registros de eventos de Windows en la categoría de registros de aplicación. Asegúrese de que el conjunto de registros de aplicación esté habilitado en el origen de eventos de GFI LanGuard.

Para habilitar el procesamiento de eventos de GFI LanGuard:

1. Abra la Consola de administración de GFI EventsManager.

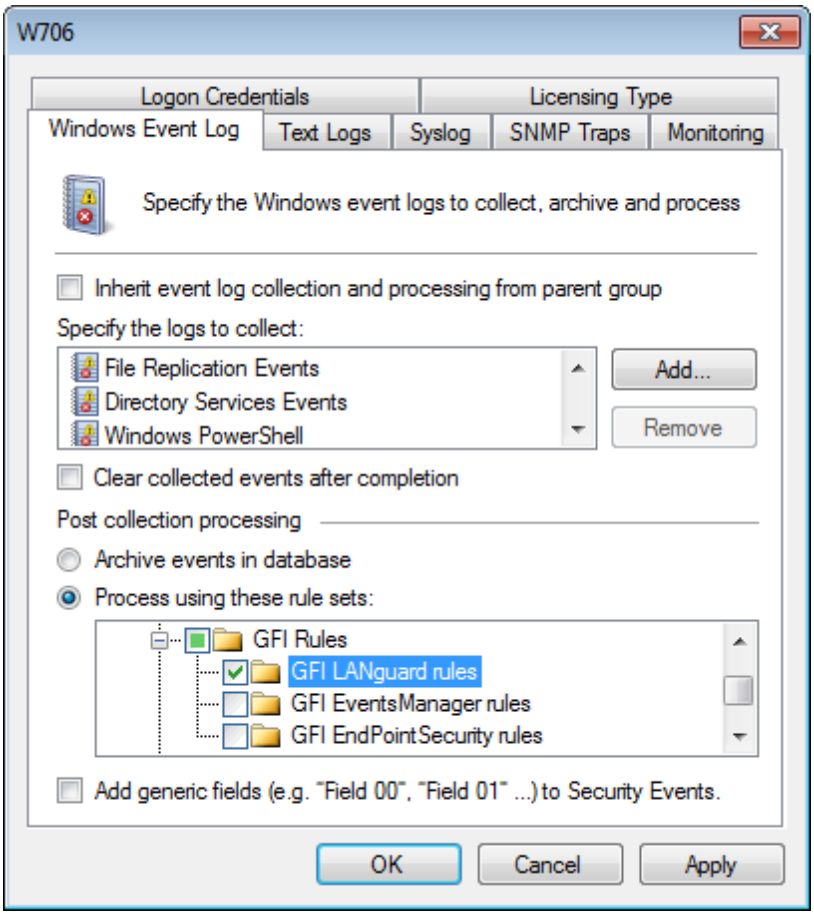
2. Haga clic en la ficha **Configuration > Event Sources**.

3. Haga clic en el origen de eventos de GFI LanGuard y seleccione **Properties**.



Captura de pantalla 85: Agregar registros de aplicación de Windows®

4. En la ficha **Windows® Event Log**, haga clic en **Add** y seleccione **Windows® Logs**. Haga clic en **Aceptar**.



Captura de pantalla 86: Agregar reglas de GFI LanGuard

5. Seleccione **Process using these rule sets**. Expanda el nodo **Windows Events >GFI Rules** y seleccione **GFI LanGuardrules**.

6. Haga clic en **OK** para aceptar.

> **Nota**
>
> GFI EventsManager tiene reglas de procesamiento de eventos integradas para eventos de GFI LanGuard que están habilitadas de forma predeterminada. Para supervisar los eventos generados por GFI LanGuard, seleccione la ficha **Status > General** y busque la sección **Critical and High Importance Events**.

> **Nota**
>
> Para configurar las reglas de procesamiento de eventos de GFI LanGuard, haga clic en la ficha **Configuration > Event Processing Rules**. En el panel izquierdo, seleccione **GFI Rules > GFI LanGuardrules**. Para obtener más información, consulte Reglas de procesamiento de eventos.

Pruebas y resolución de problemas

Para comprobar si se están generando los eventos de GFI LanGuard:

1. Abra GFI LanGuard y ejecute un análisis de auditoría de seguridad en el host local.

2. Cuando finalice el análisis, abra **Event Viewer** en **Start > Run** y escriba **eventvwr**. Presione la tecla **Enter**.

3. Vaya a Event Viewer (local) Windows Logs Application.

4. Una vez que se hayan cargados los eventos almacenados, busque una entrada con:

- Origen: GFI LanGuard
- ID de evento: 0

En caso de que el registro de eventos no esté creado, por lo general el análisis de GFI LanGuard ya se inició una vez que se modificó la clave de registro para generar los registros de eventos. Vuelva a ejecutar el análisis. O bien, asegúrese de que el valor de registro se haya creado en la ubicación correcta, puesto que la ubicación de las plataformas x86 es diferente a la de las plataformas x64.

5.7 Recopilar eventos de GFI EndPointSecurity

GFI EndPointSecurity le permite mantener la integridad de datos mediante la prevención del acceso no autorizado y la transferencia de contenido hacia y desde los siguientes dispositivos o puertos de conexión:

Tabla 38: Dispositivos compatibles con GFI EndPointSecurity

Dispositivo	Ejemplo
Puertos USB	Lectores de tarjetas flash/memoria y pen drives.
Puertos Firewire	Cámaras digitales y lectores de tarjetas Firewire
Dispositivos inalámbricos	Llaves bluetooth e infrarrojas
Unidades de disquete	Unidades de disco internas y externas (USB).
Unidades ópticas	Discos CD, DVD y Blu-ray.
Unidades magnetoópticas	Unidades internas y externas (USB).
Dispositivos de almacenamiento extraíble	Unidades de disco duro USB.
Otras unidades, como unidades Zip y unidades de cinta	Unidades internas o externas (USB/seriales/pararelas).

Nota

Para más información sobreGFI EndPointSecurity, consulte http://www.gfi.com/endpointsecurity.

Habilitar registro de GFI EndPointSecurity

De forma predeterminada, GFI EndPointSecurity genera registros con información sobre:

- El servicio de GFI EndPointSecurity
- Dispositivos conectados y desconectados de su red
- Acceso permitido o denegado por GFI EndPointSecurity a los usuarios

Para configurar las opciones de registro en GFI EndPointSecurity:

1. En la máquina que ejecuta el equipo de GFI EndPointSecurity, inicie la Consola de administración de GFI EndPointSecurity.

2. Haga clic en la ficha **Configuration > Protection Policies.**

3. En el panel izquierdo, seleccione la directiva de protección y haga clic en **Set Logging Options**.

4. Personalice los parámetros disponibles en el cuadro de diálogo Logging Option.

Nota

Para obtener más información acerca de cómo configurar las opciones de registro GFI EndPointSecurity, consulte la documentación de GFI EndPointSecurity disponible en http://www.gfi.com/products/gfi-endpointsecurity/manual.

Supervisar eventos de GFI EndPointSecurity

GFI EventsManager tiene reglas de procesamiento integradas para eventos de GFI EndPointSecurity que están habilitadas de forma predeterminada. Para supervisar los eventos generados por GFI EndPointSecurity, seleccione la ficha **Status > General** y busque la sección **Critical and High Importance Events**.

Para configurar reglas de procesamiento de eventos de GFI EndPointSecurity, haga clic en la ficha **Configuration > Event Processing Rules**. Para obtener más información, consulte Reglas de procesamiento de eventos.

6 Buscar eventos almacenados

En este capítulo, se proporciona información sobre cómo usar el Explorador de eventos. El Explorador de eventos está equipado con herramientas para llevar a cabo análisis de eventos e investigaciones forenses. También le permite desplazarse fácilmente a través de múltiples bases de datos de eventos, además de exportar eventos a bases de datos cifradas para cumplir con los requisitos legales.

Temas de este capítulo:

6.1 Desplazarse en el Explorador de eventos 126

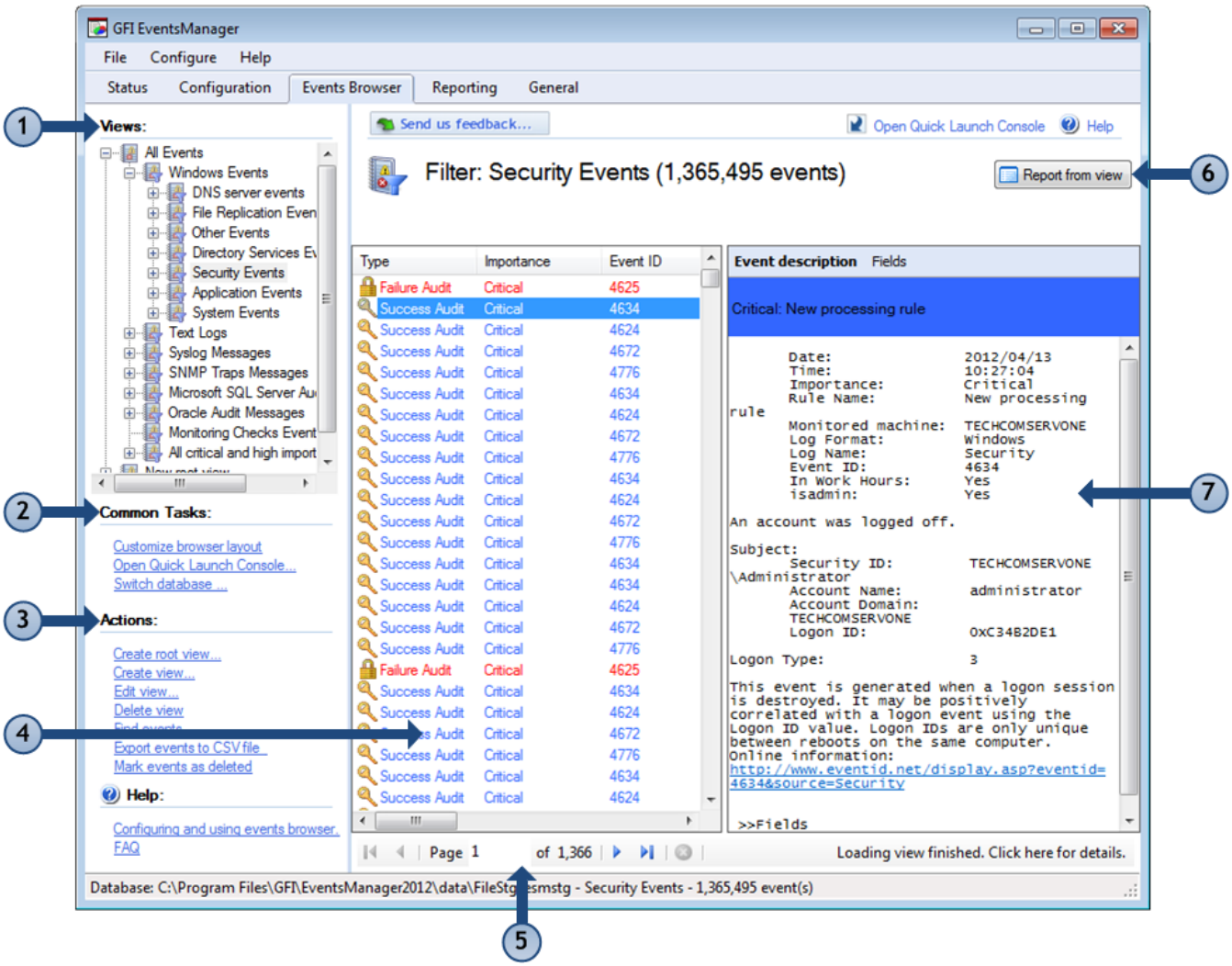
6.2 Usar el Explorador de eventos 127

6.3 Administrar vistas en el Explorador de eventos 130

6.4 Personalizar el diseño del Explorador de eventos 134

6.5 Buscar eventos desde diferentes bases de datos 136

6.1 Desplazarse en el Explorador de eventos



Captura de pantalla 87: Explorador de eventos

El Explorador de eventos se compone de las siguientes secciones:

Tabla 39: Desplazarse en el Explorador de eventos

	Sección	Descripción
1	**Views**	La sección **Views** incluye una amplia gama de vistas predefinidas. Use esta sección para ver registros específicos, como Windows® registros de eventos, registros de texto, auditorías de SQL Server® y mucho más.
2	**Common Tasks**	**Common Tasks** le permite personalizar la apariencia del Explorador de eventos y cambiar de base de datos para poder ver registros de eventos exportados o archivados.
3	**Actions**	Use la sección **Actions** para ejecutar funciones comunes relacionadas con el análisis de los registros de eventos. Esto le permite crear o editar vistas personalizadas, exportar eventos para su posterior análisis y mucho más.
4	**Events**	La sección **Events** se usa para explorar los eventos clasificados en la vista seleccionada (de la sección 1).
5	**Controles de desplazamiento**	Use los controles de desplazamiento para buscar eventos recopilados.
6	**Generación de informes**	La opción **Report from view** le permite generar informes gráficos y estadísticos basados en la vista seleccionada (de la sección 1).
7	**Panel Event Description**	El panel **Events Description** proporciona un amplio desglose del evento seleccionado (de la sección 4). Use esta sección para analizar los detalles del evento y saber cuando se generó el evento, cuál fue la causa y quién lo generó. El encabezado de codificación de colores le permite identificar rápidamente la gravedad del evento. La sección de descripción le permite cambiar de una vista a otra: » **General**: contiene la información del evento en el formato heredado que era estándar para los registros de eventos previos a Microsoft®Windows® Vista. » **Fields**: contiene una lista de información de eventos clasificados por campos. El vínculo que aparece en la descripción del evento le brinda acceso a: » Una descripción más detallada del evento » Información y vínculos que explican la causa de este tipo de evento » Consejos y sugerencias sobre cómo resolver cualquier problema existente

6.2 Usar el Explorador de eventos

El análisis de eventos es una tarea exigente; GFI EventsManager está equipado con herramientas especiales que simplifican este proceso. Use el Explorador de eventos para el análisis forense de los eventos. Todos los eventos a los que se pueden acceder con el Explorador de eventos se encuentran organizados según el tipo de registro en la sección **Views**. En las siguientes secciones, se describe cómo usar el Explorador de eventos para administrar sus eventos:

- Exportar eventos a CSV
- Crear informes a partir de vistas del explorador de eventos
- Eliminar eventos
- Buscar eventos almacenados
- Identificar reglas mediante la herramienta de búsqueda de reglas

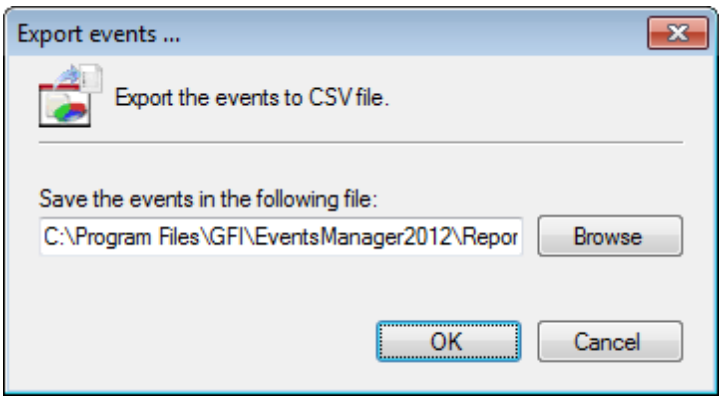
6.2.1 Exportar eventos a CSV

GFI EventsManager le permite exportar los datos de eventos a archivos CSV directamente desde el Explorador de eventos. Esto es muy práctico, especialmente cuando se requiere el posterior procesamiento de los datos del evento. Esto incluye:

- Distribución de datos de eventos clave mediante correo electrónico
- Ejecución de secuencias de comando automatizadas que convierten los datos del evento exportado de CSV a HTML para su carga en la web/intranet de la compañía
- Generación de informes de administración gráficos y datos estadísticos con herramientas nativas, como Microsoft®Excel®
- Generación de informes personalizados con aplicaciones de terceros
- Conexión de datos de eventos con aplicaciones y secuencias de comandos implementados en la empresa

Para exportar eventos a CSV:

1. En **Events Browser> Views**, haga clic con el botón secundario en una vista y seleccione **Export events**.



Captura de pantalla 88: Herramienta de exportación de eventos

2. Especifique o busque la ubicación donde se guardan los eventos exportados. Haga clic en **Aceptar**.

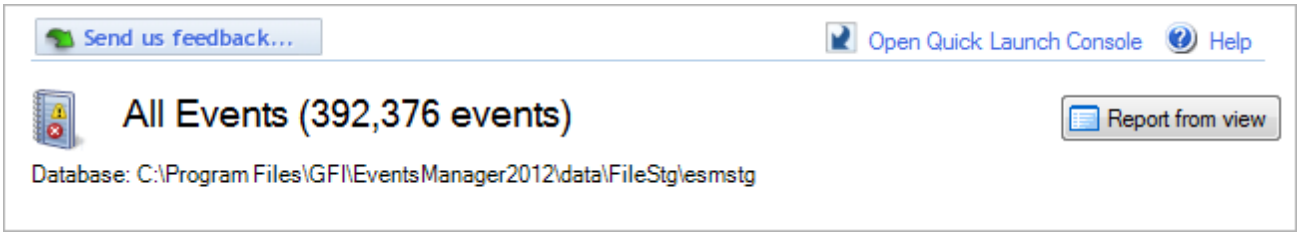
6.2.2 Crear informes a partir de vistas

GFI EventsManager le permite crear sus propios informes personalizados (con gráficos y estadísticas) basados en una vista seleccionada del Explorador de eventos.

> **Nota**
>
> GFI EventsManager envía una selección de informes predefinidos. Le recomendamos que revise los informes disponibles antes de crear nuevos informes para evitar la duplicación de informes.

Para generar un informe a partir de una vista:

1. En **Events Browser> Views**, seleccione una vista.



Captura de pantalla 89: Botón Report from view

2. En la esquina superior derecha del Explorador de eventos, haga clic en **Report from view**.

3. En el cuadro de diálogo **Create Report**, configure las opciones de las fichas que se describen a continuación:

Tabla 40: Explorador de eventos: Crear nuevo informe

Ficha	Descripción
General	Especifique el nombre del nuevo informe y agregue condiciones.
Layout	Seleccione las columnas que desea mostrar en el informe. También puede personalizar el orden de aparición.
Chart	Seleccione **Use graphical charts** para generar un informe que muestre la información en un gráfico. Los tipos de gráfico disponibles son: » Gráfico circular » Gráfico de barras » Gráfico de líneas
Schedule	Seleccione **Use schedule** para habilitar la programación de informes. Configure la fecha y frecuencia de generación para el nuevo informe.

Nota

Para obtener más información, consulte Crear informes personalizados.

6.2.3 Eliminar eventos

Al recopilar y procesar los registros de eventos de un número significativamente amplio de orígenes de eventos, se recopila una serie de registros no deseados. Para ayudar a eliminar estos registros de eventos, GFI EventsManager incluye una opción de eliminación. Cuando se eliminan los eventos:

- Se eliminan del explorador de eventos
- Ya no se incluyen en taras de exportación/importación
- Ya no se incluyen en los informes

Después de eliminar un evento, también se eliminan todos los demás eventos del mismo tipo, categoría y vista.

Importante

Antes de eliminar los registros de eventos, asegúrese de estar respetando las normas de cumplimiento legal. La eliminación de registros de eventos puede conllevar sanciones legales.

Para eliminar eventos:

1. En la ficha **Events Browser > Views**, seleccione una vista.
2. Seleccione un evento que desea eliminar. En **Actions**, haga clic en **Mark events as deleted**.
3. Haga clic en **Yes** para confirmar la eliminación o en **No** para cancelar.

Ver eventos eliminados

Los registros de eventos eliminados se almacenan en una base de datos independiente y se pueden ver desde el Explorador de eventos.

Para ver los registros de eventos eliminados:

1. Haga clic en la ficha **Events Browser**.

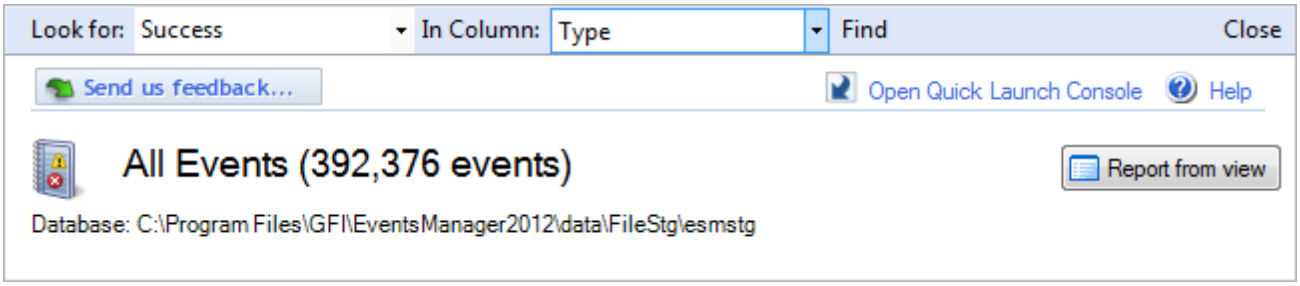
2. En el panel superior derecho, haga clic en **View deleted events**. El Explorador de eventos cambia automáticamente de base de datos.

> **Nota**
>
> Para eliminar por completo los registros de eventos de GFI EventsManager, debe ejecutar una tarea **Commit Deletion** para confirmar la eliminación en la base de datos seleccionada. Para obtener más información, consulte Confirmar eliminaciones.

6.2.4 Buscar eventos almacenados

Use la herramienta de búsqueda de eventos para buscar y localizar eventos específicos con filtros simples que se pueden personalizar. Para buscar un evento en particular:

1. Haga clic en **Events Browser > Actions > Find events**.



Captura de pantalla 90: Herramienta de búsqueda de eventos

2. Configure los parámetros de búsqueda de eventos a través de las opciones que aparecen en la parte superior del panel derecho. Para activar una búsqueda que distinga entre mayúsculas y minúsculas, haga clic en **Options** y seleccione **Match whole word**.

3. Haga clic en **Find** para iniciar la búsqueda.

6.2.5 Identificar reglas mediante la herramienta de búsqueda de reglas

GFI EventsManager le permite identificar la regla de procesamiento de eventos que provocó el registro de evento seleccionado.

Para identificar las reglas que se utilizan para un evento específico:

1. En **Events Browser**, haga clic con el botón secundario en un registro de eventos.

2. Haga clic en **Find Rule**. Esto lo llevará a la ficha **Configuration > Event Processing Rules**. Para obtener más información, consulte Reglas de procesamiento de eventos.

6.3 Administrar vistas en el Explorador de eventos

Los registros de eventos se clasifican automáticamente en carpetas diferentes, según el tipo de registro de eventos y el origen del que se generó. En GFI EventsManager, estas carpetas se denominan vistas.

GFI EventsManager incluye una lista completa de vistas que le permiten iniciar la clasificación de los registros de eventos procesados en la instalación. Se pueden crear nuevas vistas y se pueden modificar las vistas ya existentes. Las siguientes secciones proporcionan información sobre la administración de las vistas del Explorador de eventos:

- Crear vistas raíz y vistas
- Editar una vista
- Eliminar una vista

6.3.1 Crear vistas raíz y vistas

En el Explorador de eventos, GFI EventsManager le permite crear los dos tipos de vistas que se describen a continuación:

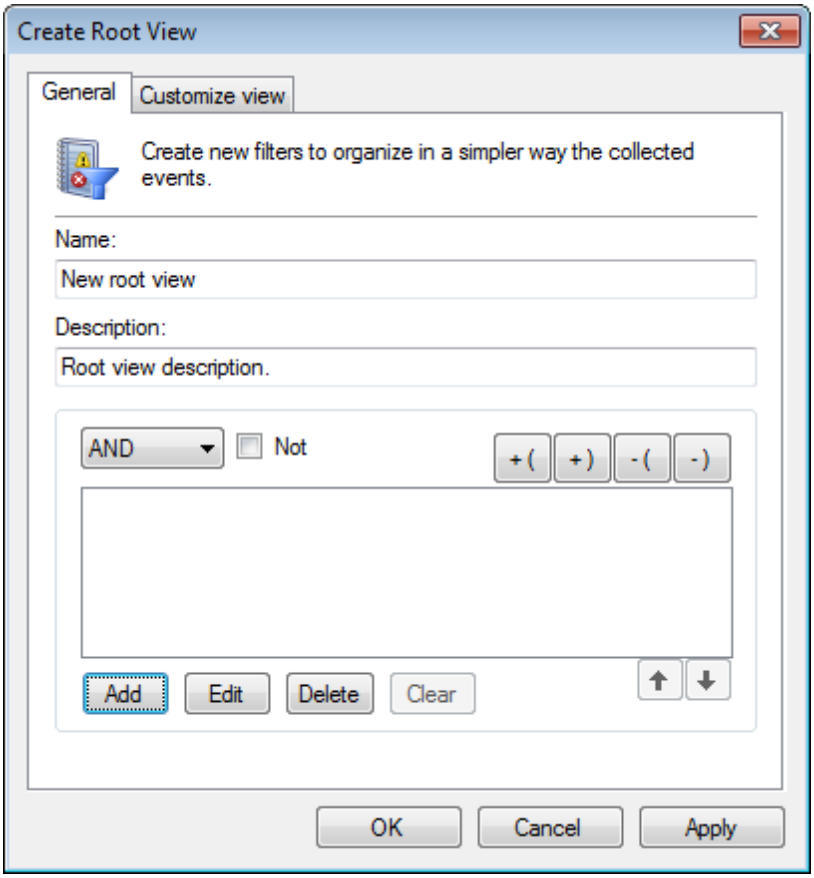
Tabla 41: Explorador de eventos: Crear una nueva vista

Vista	Descripción
Create root view…	Le permite crear vistas de primer nivel que pueden contener un número de subvistas. Esto crea un nuevo conjunto de vistas inferiores a las que se incluyen con el producto (por ejemplo: vista **All Events**).
Create view…	Le permite crear vistas dentro de las vistas raíz. Las vistas personalizadas se pueden agregar a las vistas raíz y las vistas predeterminadas.

Para crear una vista raíz/vista:

1. En **Events Browser > Actions**, haga clic en **Create root view…/Create view…**.

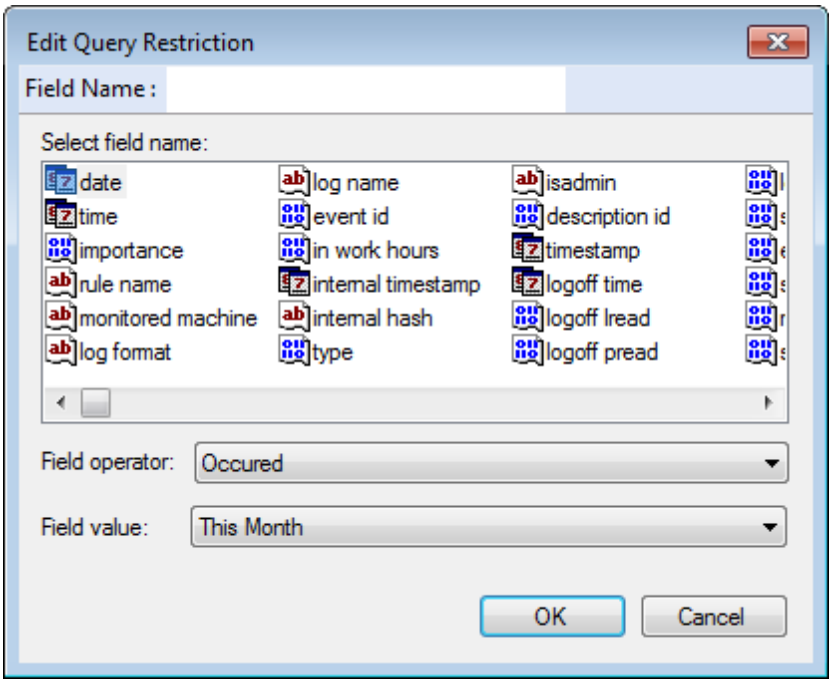
> **Nota**
>
> Ambas opciones abren el mismo cuadro de diálogo **Create view** y ambas se configuran del mismo modo. La diferencia radica en el posicionamiento de la nueva vista personalizada.



Captura de pantalla 91: Generador de vista personaliza

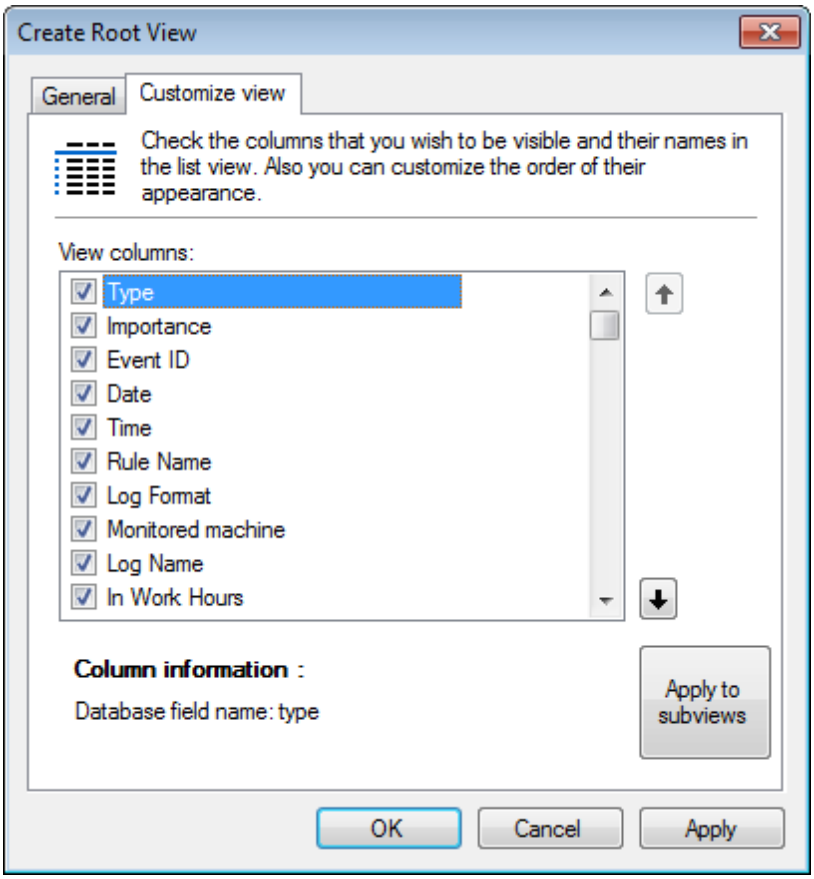
2. Escriba un nombre y una descripción para la nueva vista.

3. Haga clic en **Add** para agregar condiciones de filtro a su vista. Si no se especifican condiciones, la vista mostrará la información de cada evento que se genera.



Captura de pantalla 92: Editar restricción de vista

4. Seleccione un campo de la lista de campos disponibles y especifique los valores en **Field operator** y **Field value** para el operador y el valor del campo, respectivamente. Repita este paso hasta que se especifiquen todas las condiciones requeridas. Haga clic en **OK**. Para obtener más información, consulte Definir restricciones.

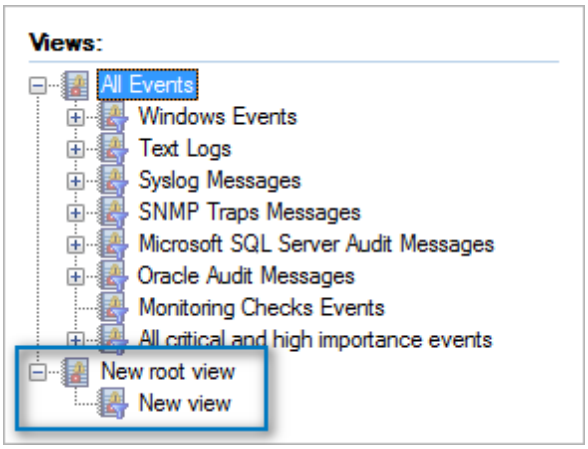


Captura de pantalla 93: Ficha Customize View

4. Haga clic en la ficha **Customize view** para seleccionar las columnas que se deben mostrar en la nueva vista personalizada. También puede organizar el orden de aparición con las teclas de flecha **Hacia arriba** y **Hacia abajo**.

5. (Opcional) Haga clic en **Apply to subviews** para aplicar las columnas seleccionadas a todas las subvistas de la vista raíz.

6. Haga clic en **Apply** y **OK**.



Captura de pantalla 94: Muestra: Vistas y vistas raíz nuevas

6.3.2 Editar una vista

1. En **Events Browser > Views**, seleccione la vista que desea editar.

2. En **Actions**, haga clic en **Edit view…**.

3. En el cuadro de diálogo View Properties, agregue, edite o elimine las condiciones de acuerdo con sus necesidades.

6.3.3 Eliminar una vista

1. En **Events Browser > Views**, seleccione la vista que desea eliminar.

2. En **Actions**, haga clic en **Delete view**. O bien, haga clic derecho en la vista que desea eliminar y seleccione **Delete view**.

6.4 Personalizar el diseño del Explorador de eventos

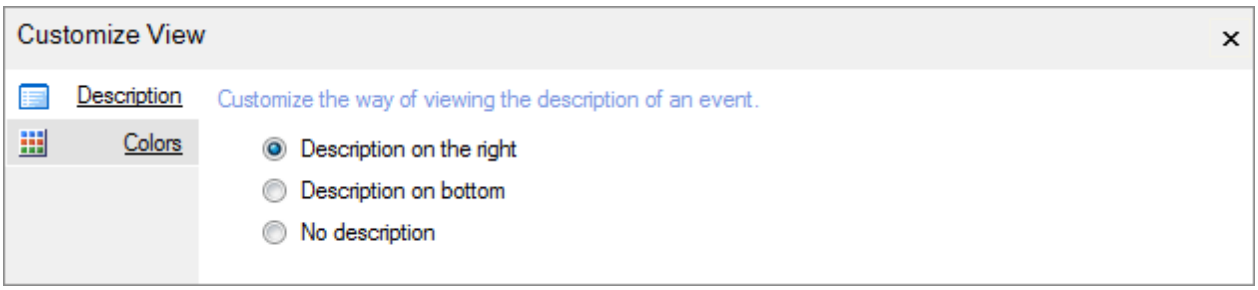
GFI EventsManager le permite personalizar el Explorador de eventos de acuerdo con sus preferencias. Puede cambiar la posición del panel de descripción, además de modificar las opciones de codificación de colores del registro de eventos que se usa para facilitar la identificación de los eventos importantes. Las siguientes secciones le proporcionan información acerca de cómo personalizar el Explorador de eventos:

- Personalizar la posición de descripción
- Opciones de codificación de colores de eventos

6.4.1 Personalizar la posición de descripción

Para cambiar la posición del panel de descripción de un evento:

1. En **Events Browser > Common Tasks**, haga clic en **Customize browser layout > Description**.



Captura de pantalla 95: Personalizar la descripción del explorador

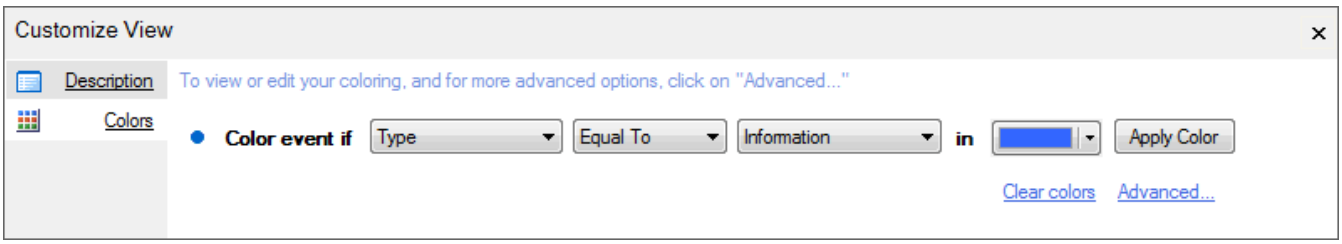
2. Seleccione una de las opciones que se describen a continuación:

Tabla 42: Descripción de las posiciones del panel

Opción	Descripción
Description on the right	Permite colocar el panel de descripción a la derecha de la lista de eventos.
Description on bottom	Permite colocar el panel de descripción en la parte inferior de la lista de eventos.
No description	Elimina el panel de descripción.

6.4.2 Opciones de codificación de colores de eventos

Use la herramienta de codificación de colores para teñir los eventos clave de un color particular. De este modo, los eventos requeridos son más fáciles de localizar durante la exploración de eventos.



Captura de pantalla 96: Configurar la codificación de colores

Para asignar una codificación de colores a un evento específico:

1. En **Events Browser > Common Tasks**, seleccione **Customize browser layout > Colors**.

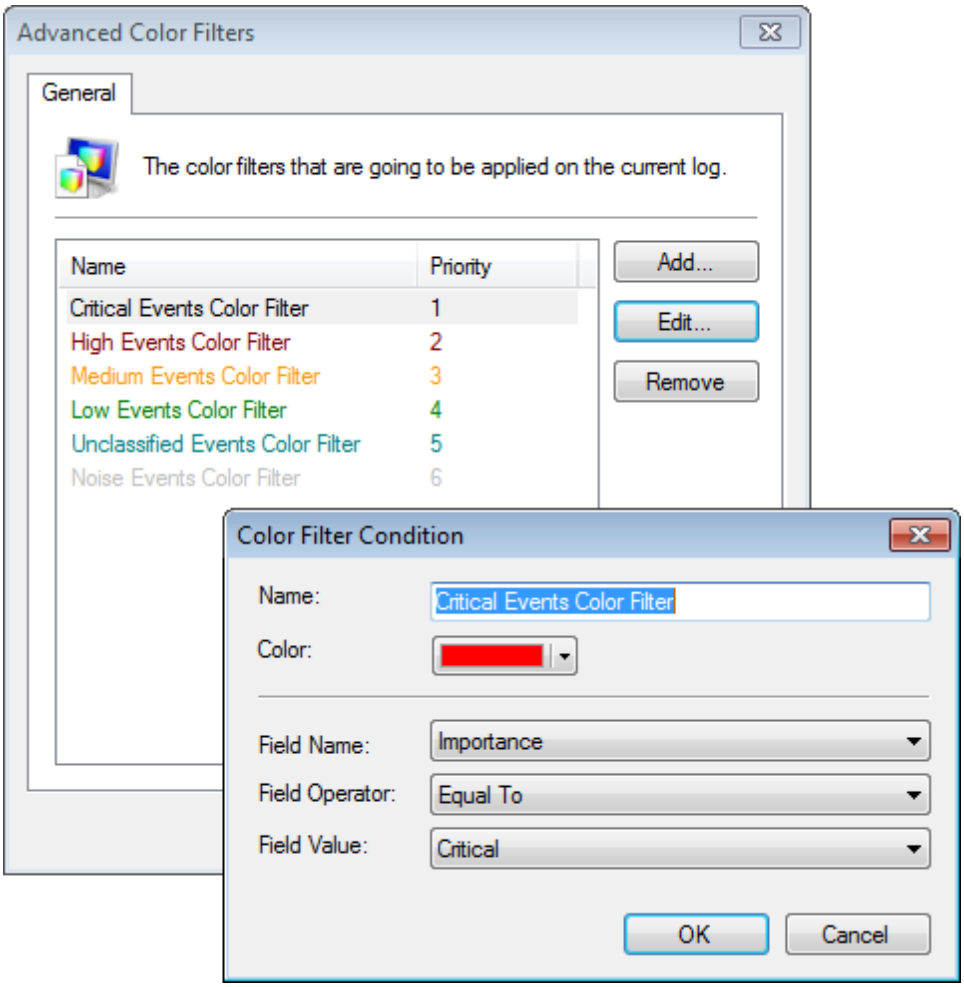
2. Especifique los parámetros de filtrado de eventos, incluso el color que se aplicará a los eventos tamizados.

3. Haga clic en **Apply Color**.

> **Nota**
>
> Use la opción **Clear color** para borrar la configuración del color.

Para asignar diferentes codificaciones de colores a varios eventos:

1. En **Events Browser > Common tasks** seleccione **Customize view > Colors > Advanced…**.



Captura de pantalla 97: Filtro de color avanzado

2. Haga clic en el botón **Add**. Especifique el nombre del filtro y configure los parámetros de filtro de eventos.

3. Haga clic en **Aceptar**.

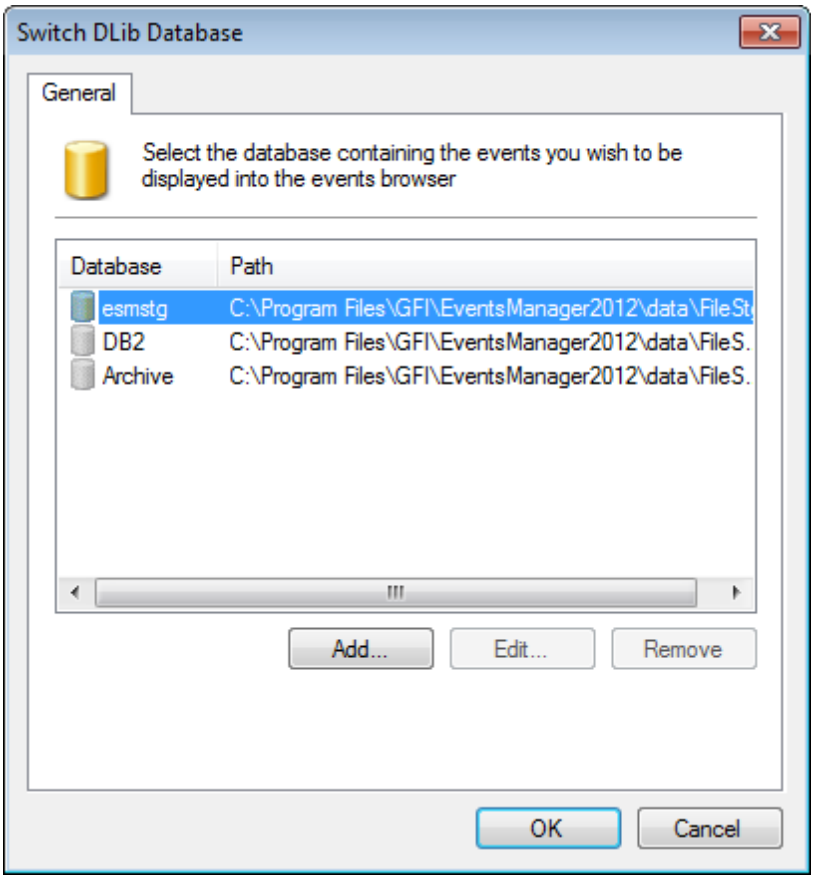
4. Repita el proceso hasta que se hayan configurado todas las condiciones de filtro de eventos requeridas. Haga clic en **Aceptar**.

6.5 Buscar eventos desde diferentes bases de datos

GFI EventsManager le permite cambiar de bases de datos. Use esta función para buscar eventos que se exportaron o archivaron para su posterior análisis o que se almacenaron en diferentes bases de datos.

Para cambiar de bases de datos:

1. Haga clic en **Events Browser > Common Tasks > Switch database**.



Captura de pantalla 98: Cuadro de diálogo Switch database

2. Seleccione la base de datos de la lista de bases de datos y haga clic en **OK**.

> **Nota**
>
> Puede hacer clic en **Add...** para especificar una ruta y un nombre único para crear una nueva base de datos. Haga clic en **Edit...** para editar la información especificada.

7 Supervisión de actividades

En este capítulo, se brinda información acerca de la supervisión de los procesos de recopilación de eventos. La ficha **Status** es un panel donde se muestra el estado deGFI EventsManager, así como la información estadística relacionada con los eventos recopilados, procesados y archivados. El monitor de estado se compone de tres diferentes vistas del panel: Vista **General**, vista **Job Activity** y vista **Statistics**.

Temas de este capítulo:

7.1 Vista de estado general 137

7.2 Vista de actividad de tareas 141

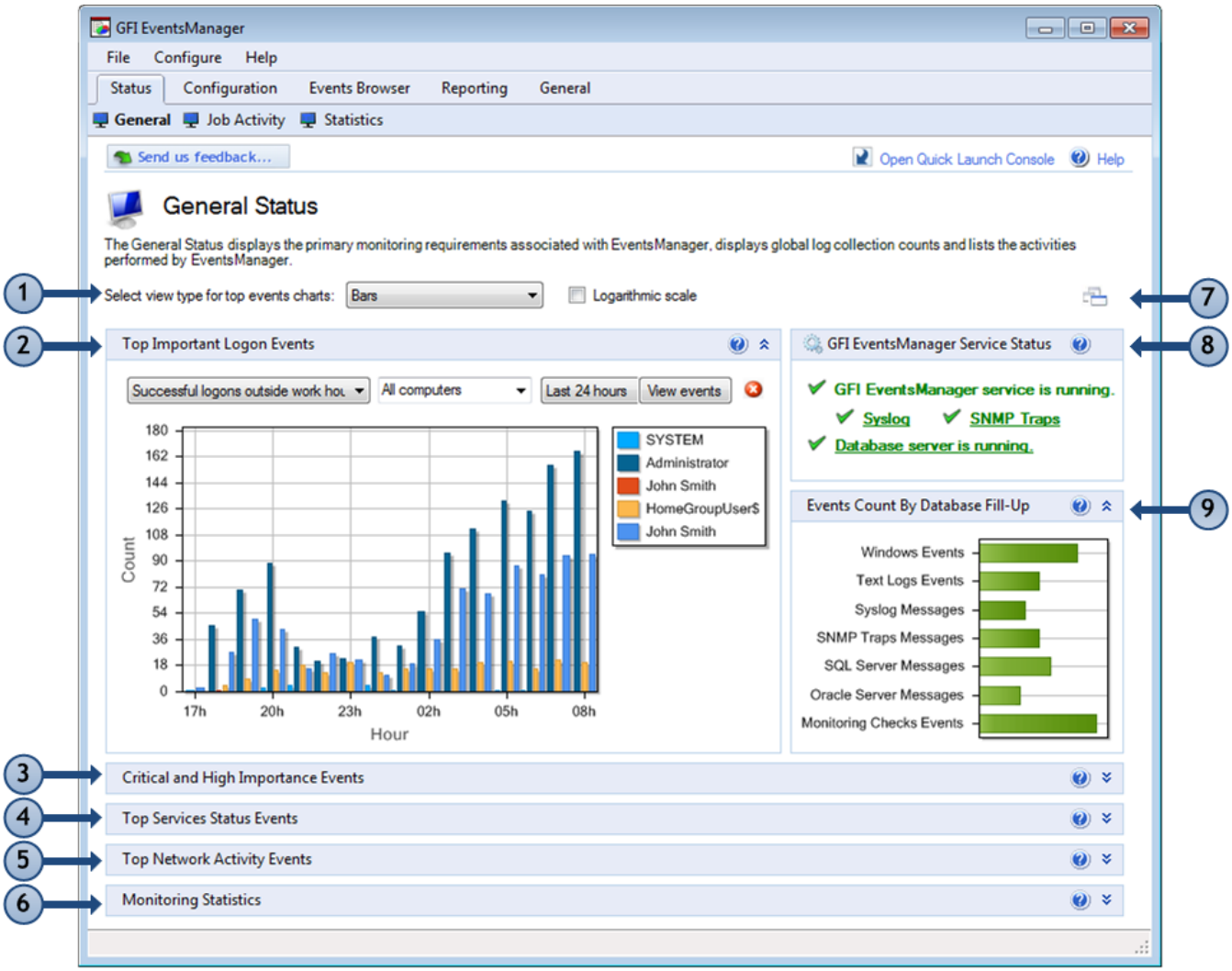
7.3 Vista de estadísticas 143

7.1 Vista de estado general

Esta vista de estado general se utiliza para:

- Ver el estado del motor de procesamiento de eventos de GFI EventsManager
- Acceder a información de estadísticas, como el número de eventos de inicio de sesión, los eventos críticos y los eventos de estado de servicio.

Para acceder a la vista **General**, vaya a la ficha **Status > General**.



Captura de pantalla 99: Estado de GFI EventsManager: Vista general

La vista general consta de las secciones que se describen a continuación:

Tabla 43: Supervisión de estado: Secciones de vista general

Sección	Descripción
1	Utilice esta sección para seleccionar el tipo de gráfico de los eventos principales.
2	La sección **Top Important Log Events** proporciona información estadística sobre: » Los primeros 10 eventos de inicio de sesión con éxito fuera de horas de trabajo » Los primeros 10 eventos de inicio de sesión importantes en horas de trabajo » Los primeros 10 eventos de inicio de sesión fallidos. Los eventos en esta sección se filtran por: » **Machine**: Seleccione un equipo o ingrese un nombre de equipo en la lista desplegable » **Period**: El período de tiempo en que ocurrieron los hechos (Última hora, Últimas 24 horas, Últimos 7 días o una fecha específica).

Sección	Descripción
3	La sección **Critical and High Importance Events** proporciona información estadística/gráfica sobre eventos críticos recopilados de todos los orígenes de eventos. Este gráfico muestra las reglas de procesamiento de eventos que recopilan y procesan los eventos durante un período determinado. En las listas desplegables, seleccione el tipo de información que desea mostrar. Seleccione una de las siguientes opciones: » **Grouping**: Determina cómo se agrupan los eventos; como eventos, equipos, grupos de equipos, eventos/equipos o grupos de eventos/equipos. » **Event type**: Seleccione el tipo de datos que desea mostrar (Windows®, registros de texto, syslog, captura SNMP, registros de supervisión activa, auditoría de SQL y Oracle) » **Alert type**: Especifique la gravedad de la alerta, como todas las alertas, críticas o altas » **Period**: Especifique el período de tiempo en que ocurrieron los hechos (Última hora, Últimas 24 horas, Últimos 7 días o una fecha específica). **NOTA** Esta sección también muestra los resultados de vulnerabilidad supervisados por GFI LanGuard. **NOTA** Para obtener información detallada sobre los diferentes tipos de eventos importantes que se muestran en esta vista, descargue la Guía de supervisión de seguridad y planificación de detección de ataques de Microsoft® en http://go.gfi.com/?pageid=esm_smad_plan.
4	**Top Service Status Events** muestra los primeros 10 servicios que causaron el evento seleccionado. Un servicio puede generar eventos cuando: » Termina con un error » No se puede cargar » No se puede iniciar » Se agota el tiempo de espera » Se detiene » Se inicia El gráfico muestra la frecuencia de estos eventos según el tipo de servicio o el equipo que genera el evento. Seleccione un equipo o servicio de las listas desplegables o especifique los criterios necesarios para personalizar los resultados gráficos. **Nota** Para recopilar información de los servicios, los orígenes de eventos deben tener activada la política Audit system events. Para obtener más información, consulte Activar permisos de orígenes de eventos manualmente (página 339).

Sección	Descripción
5	La sección **Top Network Activity Events** muestra los detalles de las primeras 10 actividades de la red (entrantes y salientes). La actividad de la red se compone de todo tipo de tráfico generado por varios protocolos, incluso SMTP, HTTP, FTP y MSN. Las actividades de la red que se muestran se pueden filtrar por: » Aplicaciones » Direcciones de origen » Direcciones de destino » Equipos » Puertos » Usuarios Seleccione los parámetros de las listas desplegables o ingrese los valores para filtrar el tipo de gráfico que se muestra. **Nota** La actividad de la red que se muestra en el gráfico solamente se aplica a equipos con Microsoft®Windows® Vista o posterior. **Nota** Para recopilar las actividades de la red, los orígenes de eventos deben tener activadas las opciones Object auditing y Process tracking. Para obtener más información, consulte Activar permisos de orígenes de eventos manualmente.
6	La sección **Monitoring Statistics** muestra información de estado acerca de la supervisión activa que usted está ejecutando en los orígenes de eventos. La información que se muestra en esta sección se actualiza cada 20 segundos y le proporciona: » Nombre de la comprobación » Recuento exitoso/fallido » Número de eventos generados » Fecha y hora de la comprobación » Tipo de comprobación Seleccione una fila y haga clic en **View Events** para ver los registros relacionados que se generaron cuando la comprobación de completó correctamente/incorrectamente.
7	Haga clic en el ícono **Arrange Window** para ajustar automáticamente todos los gráficos de la Consola de administración.
8	El **estado de servicio** de GFI EventsManager se utiliza para ver: » El estado de funcionamiento del servicio/motor de procesamiento de eventos de GFI EventsManager » El estado de funcionamiento del servidor Syslog » El estado de funcionamiento del servidor de capturas SNMP » El estado de funcionamiento del servidor de base de datos actualmente en uso por GFI EventsManager. **Nota** Haga clic en el nombre del servicio para editar la configuración del servicio. **Nota** Haga clic en **Database server is running** para cambiar de base de datos. Para obtener más información, consulte Cambiar de bases de datos de almacenamiento de archivos.

Sección	Descripción
9	**Events Count By Database Fill-Up** muestra: » Las barras horizontales representan el número de eventos almacenados en el back-end de base de datos, ordenados por tipo de registro de eventos » La fecha y hora de la última copia de seguridad » La fecha y hora de la siguiente copia de seguridad programada El color de la barra cambia de verde a rojo a medida que la base de datos se llena con eventos.

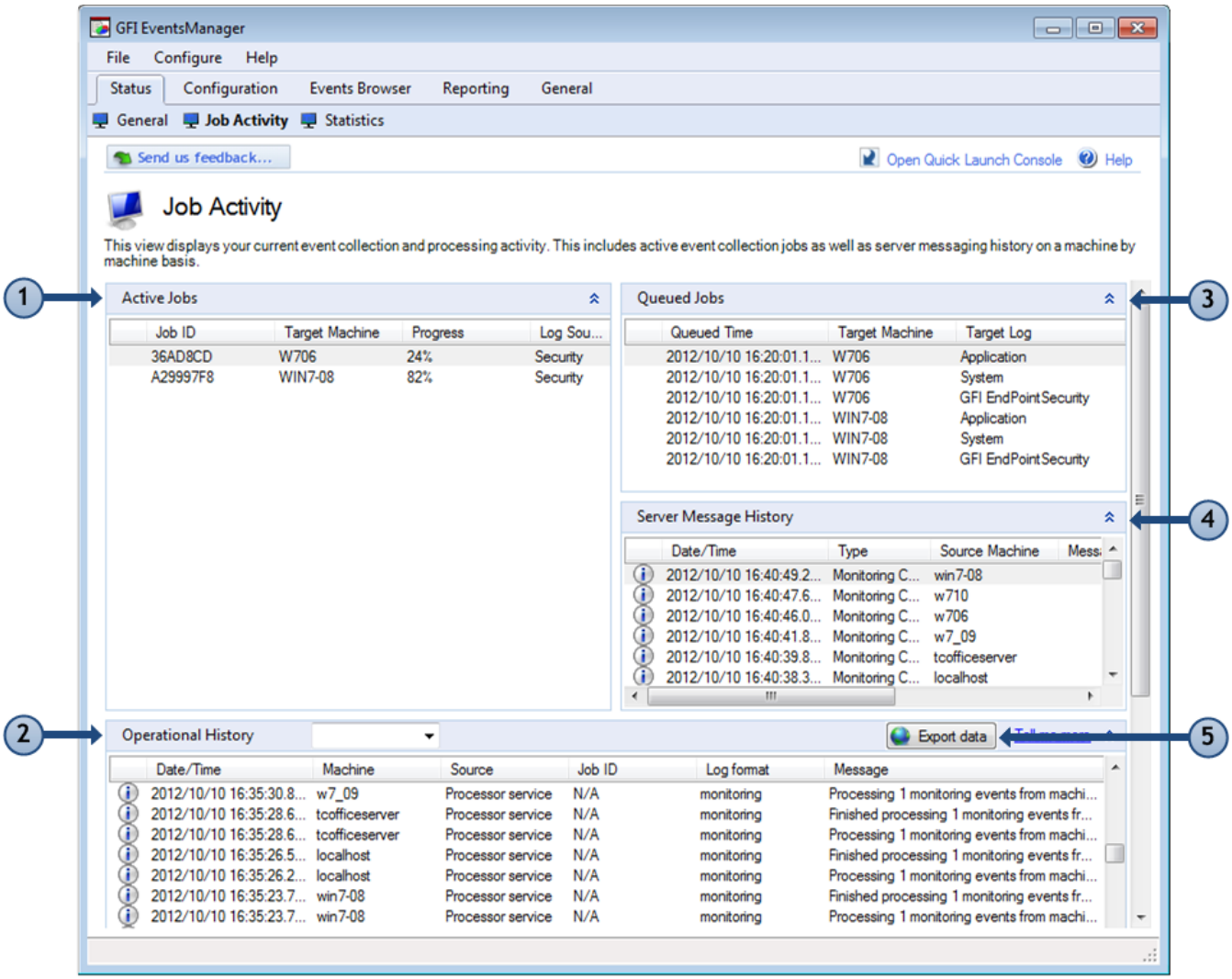
Nota

Haga doble clic en el gráfico para abrir el gráfico en una nueva ventana. Cuando se selecciona un gráfico 3D, la nueva ventana le permite rotar, hacer zoom o cambiar el tamaño del gráfico. Utilice el botón **Export to image** para exportar el gráfico.

7.2 Vista de actividad de tareas

Esta vista muestra la recopilación de eventos actuales y la actividad de procesamiento. Esto incluye tareas activas de recopilación de eventos, así como el historial de mensajes del servidor máquina por máquina.

Para acceder a la vista **Job Activity**, vaya a la ficha **Status > Job Activity**.


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
General Job Activity Statistics
Send us feedback...
Open Quick Launch Console Help
Job Activity
This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.
1
Active Jobs
Job ID Target Machine Progress Log Sou...
36AD8CD W706 24% Security
A29997F8 WIN7-08 82% Security
3
Queued Jobs
Queued Time Target Machine Target Log
2012/10/10 16:20:01.1... W706 Application
2012/10/10 16:20:01.1... W706 System
2012/10/10 16:20:01.1... W706 GFI EndPointSecurity
2012/10/10 16:20:01.1... WIN7-08 Application
2012/10/10 16:20:01.1... WIN7-08 System
2012/10/10 16:20:01.1... WIN7-08 GFI EndPointSecurity
4
Server Message History
Date/Time Type Source Machine
2012/10/10 16:40:49.2... Monitoring C... win7-08
2012/10/10 16:40:47.6... Monitoring C... w710
2012/10/10 16:40:46.0... Monitoring C... w706
2012/10/10 16:40:41.8... Monitoring C... w7_09
2012/10/10 16:40:39.8... Monitoring C... tcofficeserver
2012/10/10 16:40:38.3... Monitoring C... localhost
2
Operational History
Export data
5
Date/Time Machine Source Job ID Log format Message
2012/10/10 16:35:30.8... w7_09 Processor service N/A monitoring Processing 1 monitoring events from machi...
2012/10/10 16:35:28.6... tcofficeserver Processor service N/A monitoring Finished processing 1 monitoring events fr...
2012/10/10 16:35:28.6... tcofficeserver Processor service N/A monitoring Processing 1 monitoring events from machi...
2012/10/10 16:35:26.5... localhost Processor service N/A monitoring Finished processing 1 monitoring events fr...
2012/10/10 16:35:26.2... localhost Processor service N/A monitoring Processing 1 monitoring events from machi...
2012/10/10 16:35:23.7... win7-08 Processor service N/A monitoring Finished processing 1 monitoring events fr...
2012/10/10 16:35:23.7... win7-08 Processor service N/A monitoring Processing 1 monitoring events from machi...

Captura de pantalla 100: Estado de GFI EventsManager: Vista de actividad de tareas

La información proporcionada en esta vista se divide en las siguientes secciones específicas:

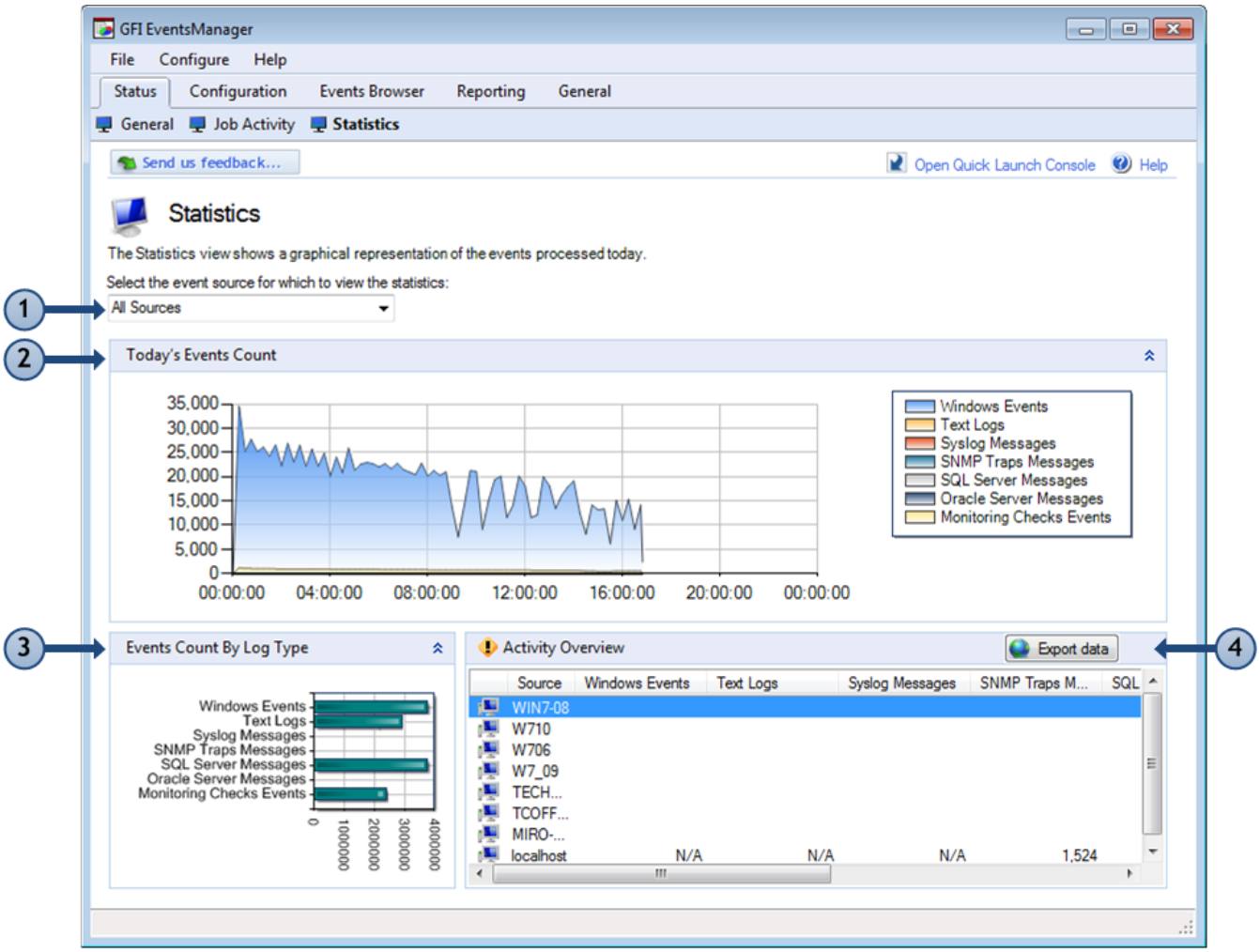
Tabla 44: Supervisión de estado: Vista de actividad de tareas

Sección	Descripción
1	La sección **Active Jobs** proporciona una lista de todas las tareas de recopilación de eventos que se llevan a cabo en cada origen de eventos/máquina. La información proporcionada incluye el progreso de la tarea, así como el origen del registro del que se están recopilando eventos.
2	La sección **Operational Histoy** muestra un seguimiento de las auditorías de las operaciones de recopilación de eventos ejecutadas por GFI EventsManager. La información proporcionada incluye los errores y los mensajes de información generados durante el proceso de recopilación de eventos, así como el nombre del archivo de registro que se estaba procesando en el origen del evento. **NOTA** Los registros del historial operativo se pueden exportar al utilizar el botón Export data. Para obtener más información, consulte Generar informes.
3	La sección **Queued Jobs** proporciona una lista máquina por máquina de todas las tareas de recopilación de eventos pendientes. La información proporcionada incluye el origen de eventos de los cuales se recopilarán los eventos, así como el tiempo de espera y el tipo de registro que se debe recopilar.
4	La sección **Server Message History** muestra una lista de todos los mensajes del servidor (capturas SNMP y Syslog) que recibió GFI EventsManager. La información proporcionada incluye el número total de mensajes enviados por cada origen de evento, el número de mensajes y la fecha/hora en que se recibió el último mensaje.
5	Haga clic en **Export data** para generar informes del historial operativo.

7.3 Vista de estadísticas

La vista **Statistics** se usa para mostrar las estadísticas y tendencias de actividad de eventos diarios de un equipo en particular o de toda la red.

Para acceder a la vista **Statistics**, vaya a la ficha **Status > Statistics**.



Captura de pantalla 101: Estado de GFI EventsManager: Vista de estadísticas

La información proporcionada en esta vista se divide en las siguientes secciones específicas:

Tabla 45: Supervisión de estado: Vista de estadísticas

Sección	Descripción
1	Use este menú desplegable para seleccionar qué información se muestra. Elija entre **All sources** o seleccione orígenes específicos para ver su información según corresponda.
2	**Today's Events Count** representa gráficamente la tendencia diaria de recopilación de eventos máquina por máquina, así como de red en red. Se usa una codificación por color para diferenciar entre eventos de Windows®, registros de texto, registros de supervisión activa, syslogs y capturas SNMP.
3	**Events Count By Log Type** representa el número de eventos de Windows®, registros de texto, capturas SNMP y syslogs que recopila GFI EventsManager de un equipo o de una red en particular.

Sección	Descripción
4	La sección **Activity Overview** proporciona información sobre: » El número total de eventos de Windows®, registros de texto, registros de supervisión activa, capturas SNMP y syslogs que se procesaron máquina por máquina. » La fecha/hora de la última recopilación de eventos que se realizó en cada máquina. Haga clic en **Export data** para generar informes de descripción general de las actividades.

8 Generación de informes

En este capítulo, se proporciona información sobre el motor de informe integral de GFI EventsManager. Viene con una serie de informes, incluidos los informes de nivel técnico y ejecutivo, que muestran información gráfica y estadísticas en función del hardware y software administrados por GFI EventsManager.

Temas de este capítulo:

8.1 Desplazarse por la ficha Reports 146

8.2 Informes disponibles 147

8.3 Administrar informes 149

8.4 Crear un informe raíz 151

8.5 Crear informes personalizados 157

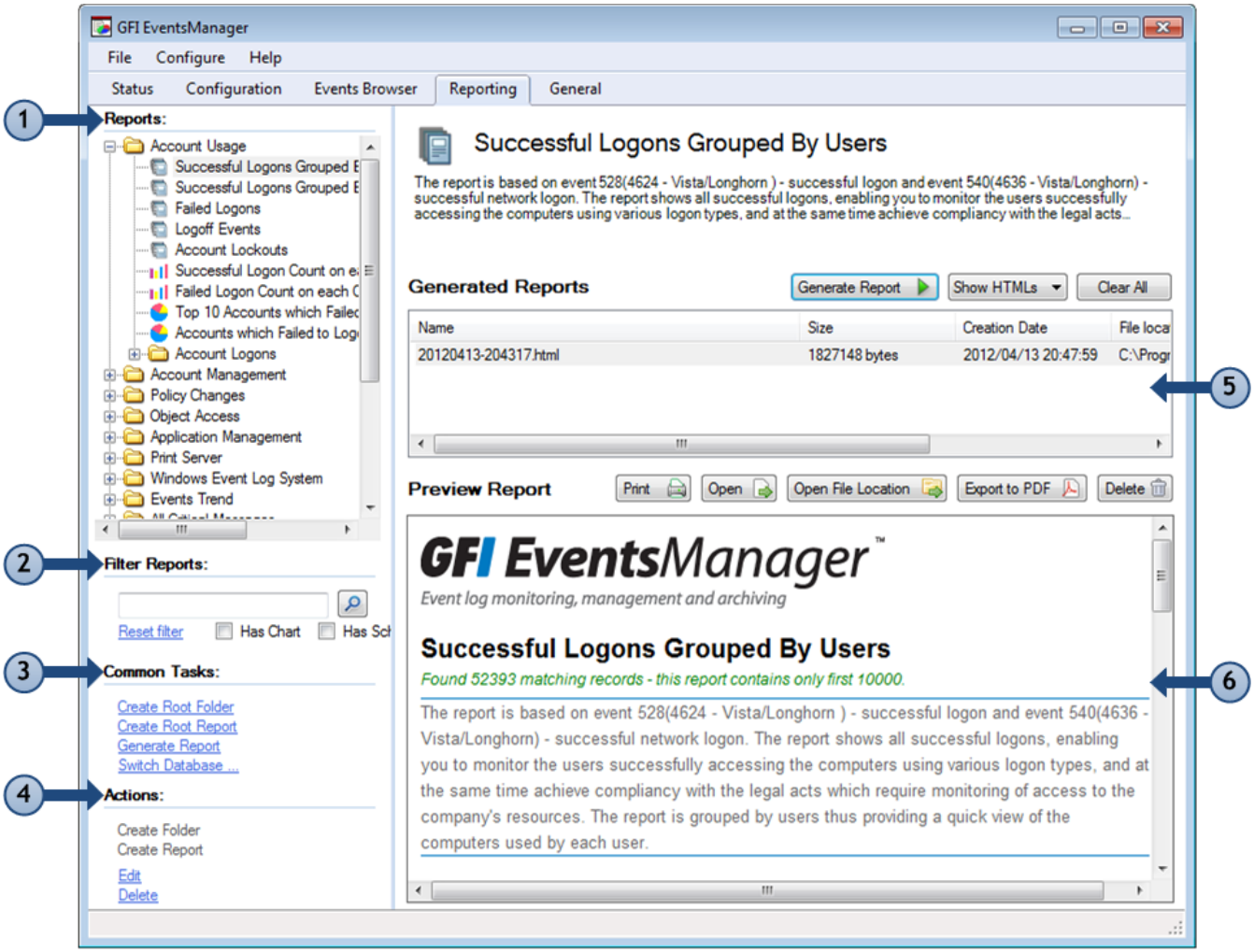
8.6 Generar informes 164

8.7 Analizar informes 174

8.8 Definir encabezados de columna 175

8.9 Personalizar informes HTML 176

8.1 Desplazarse por la ficha Reports


GFI EventsManager
File
Configure
Help
Status
Configuration
Events Browser
Reporting
General
1
Reports:
Account Usage
Successful Logons Grouped E
Successful Logons Grouped E
Failed Logons
Logoff Events
Account Lockouts
Successful Logon Count on e
Failed Logon Count on each C
Top 10 Accounts which Failed
Accounts which Failed to Log
Account Logons
Account Management
Policy Changes
Object Access
Application Management
Print Server
Windows Event Log System
Events Trend
2
Filter Reports:
Reset filter
Has Chart
Has Sch
3
Common Tasks:
Create Root Folder
Create Root Report
Generate Report
Switch Database ...
4
Actions:
Create Folder
Create Report
Edit
Delete
Successful Logons Grouped By Users
The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts...
Generated Reports
Generate Report
Show HTMLs
Clear All
Name
Size
Creation Date
File loca
20120413-204317.html
1827148 bytes
2012/04/13 20:47:59
C:\Progr
5
Preview Report
Print
Open
Open File Location
Export to PDF
Delete
GFI EventsManager
Event log monitoring, management and archiving
Successful Logons Grouped By Users
Found 52393 matching records - this report contains only first 10000.
The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.
6

Captura de pantalla 102: Desplazarse por la interfaz de informes

La ficha Reporting contiene las siguientes secciones:

Tabla 46: Desplazarse por la ficha Reporting

Sección	Descripción
1	La sección **Reporting** contiene todos los informes predefinidos que vienen con el producto. Use esta sección para organizar y generar diversos informes, desde técnicos hasta ejecutivos.
2	Encuentre informes rápidamente con las opciones de filtro disponibles. A través de las opciones incluidas en **Filter Reports**, puede buscar informes que contengan gráficos y que se generan en función de una programación.
3	La sección **Common Tasks** le permite iniciar rápidamente operaciones típicas, como la creación de vistas de carpeta e informes para organizar los informes y generar informes.
4	En **Actions**, puede crear, editar o eliminar informes según sus necesidades.
5	Use la sección **Generated Reports** para ver el historial de un informe seleccionado (Sección 1). Esto le permite volver a generar y exportar el informe en formato HTML o en PDF.
6	La sección **Preview Report** le brinda una vista de un informe seleccionado que generó. Use los botones de control Print, Open, Export o Delete reports directamente en esta sección para imprimir, abrir, exportar o eliminar informes, respectivamente.

8.2 Informes disponibles

La amplia lista de informes de GFI EventsManager contiene informes para diversos requisitos diseñados para facilitar la presentación de informes tanto como sea posible. Las siguientes categorías de informes se incluyen de forma predeterminada en GFI EventsManager. GFI EventsManager permite el uso de los informes existentes como plantillas para crear los suyos propios. Cada categoría en la tabla de abajo contiene una serie de informes que se pueden utilizar como están o que se pueden personalizar para satisfacer sus necesidades:

Tabla 47: Informes disponibles

Categoría	Description
Account Usage	Utilice los informes de esta categoría para identificar los problemas de inicio de sesión del usuario. Los detalles de los eventos que se muestran en estos informes incluyen inicios de sesión de usuario exitosos/fallidos y cuentas de usuarios bloqueadas.
Account Management	Utilice los informes de esta categoría para generar un resumen gráfico de los eventos importantes que tuvieron lugar en toda la red. Los detalles de los eventos que se muestran en estos informes incluyen cambios en el usuario y cuentas del equipo, así como cambios en las directivas de grupo de seguridad.
Policy Changes	Utilice los informes de esta categoría para identificar cambios de directivas efectuados en la red.
Object Access	Utilice los informes de esta categoría para identificar los problemas de acceso a objetos. Los detalles de los eventos que se muestran en estos informes incluyen el acceso y los objetos exitosos/fallidos que se eliminaron.
Application Management	Utilice los informes de esta categoría para identificar las aplicaciones defectuosas y los problemas de instalación y eliminación de aplicaciones. Los detalles de los eventos que se muestran en estos informes incluyen las aplicaciones que se instalaron o eliminaron, así como las aplicaciones que fallan y no responden.
Print Server	Utilice los informes de esta categoría para visualizar los detalles relacionados con los eventos de impresión. Los detalles proporcionados en estos informes incluyen documentos que se imprimieron, los usuarios que activaron el evento de impresión y la fecha/hora en que tuvo lugar la operación de impresión.
Windows Event Log System	Utilice los informes de esta categoría para identificar errores de auditoría y los problemas importantes del registro de eventos de Windows®. Los datos facilitados en estos informes incluyen el inicio y la detención de los servicios de registro de eventos y operaciones de borrado de registro, así como los errores generados durante el registro de eventos.
Events Trend	Utilice los informes de esta categoría para mostrar la información estadística relacionada con la generación de eventos. Los gráficos proporcionados incluyen los 10 equipos y usuarios con más eventos. Otros informes proporcionan recuentos de eventos en base a toda la red, así como en base a equipo por equipo. Los informes de esta categoría pueden ser generados por cada intervalo principal: por hora, día, semana o mes.
All Critical	Utilice los informes de esta categoría para mostrar la información relacionada con los eventos críticos de Windows®, Syslog, registros de texto, eventos personalizados, capturas SNMP y eventos de auditoría de SQL Server®. Los gráficos facilitados incluyen los 10 eventos más críticos.
Miscellaneous, Customizable	Utilice los informes de esta categoría para generar informes que ofrecen una amplia personalización. Estos pueden ser usados para generar informes basados en cualquier registro de eventos de Windows®, usando condiciones de filtrado y modos de agrupación que no están cubiertos por los otros informes predeterminados.
PCI DSS Compliance / GCSx Code of Connection Requirements / SOX Compliance / HIPAA Compliance / GLBA Compliance	Utilice los informes de estas categorías para generar informes de normas de cumplimiento legal.
General and Security Requirements	Utilice los informes de esta categoría para generar varios informes requeridos por varios códigos de conexión GCSx.

Categoría	Description
LOGbinder SP reports	Utilice los informes de esta categoría para generar informes relacionados con los eventos de auditoría de Microsoft® SharePoint®.

8.3 Administrar informes

Los informes están organizados en una estructura de árbol que le permite encontrar y generar el informe requerido fácilmente. GFI EventsManager incluye varias opciones que le permiten mantener fácilmente la estructura de los informes a medida que aumenta el número de informes con el tiempo.

Esta sección contiene información acerca de:

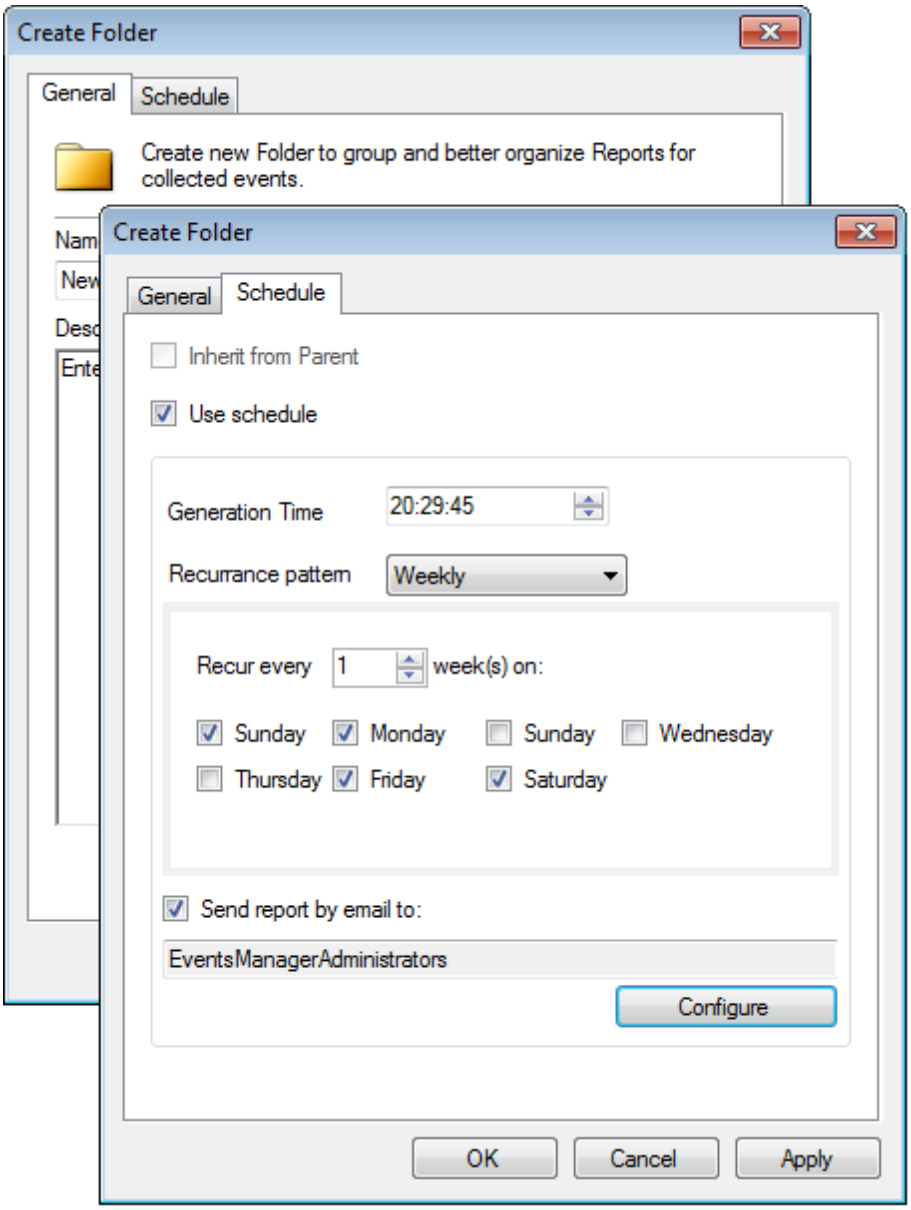
- Crear una carpeta raíz
- Crear una carpeta
- Crear un informe raíz
- Crear informes personalizados
- Definir encabezados de columna

8.3.1 Crear una carpeta raíz

Las carpetas raíz son las carpetas de nivel superior que pueden contener una o más subcarpetas o informes.

Para crear una carpeta raíz:

1. En la ficha **Reporting > Common Tasks**, haga clic en **Create Root Folder**.



Captura de pantalla 103: Cuadro de diálogo Create Report Folder

2. En la ficha **General**, especifique un nombre y una descripción (opcional) para la nueva carpeta.

3. Haga clic en la ficha **Schedule** y seleccione **Use schedule** para configurar una programación para los informes incluidos en esta nueva carpeta. Configure las opciones que se describen a continuación:

Tabla 48: Crear carpeta de informes: Opciones de programación

Opción	Description
Inherit from Parent	Seleccione esta opción cuando la nueva carpeta sea parte de una carpeta raíz cuya programación ya está configurada.
Use schedule	Seleccione **Use Schedule** para habilitar la programación de los informes contenidos en la nueva carpeta.
Generation time	Especifique el tiempo en que los informes se generan.
Recurrence pattern	Especifique la frecuencia de generación de informes. Seleccione entre el patrón **Daily**, **Weekly** o **Monthly** y configure los parámetros diarios, semanales o mensuales, respectivamente.

Opción	Description
Send report by email to	Seleccione esta opción para habilitar las notificaciones de correo electrónico. Haga clic en Configure para seleccionar los usuarios en el diálogo Select users and groups... **NOTA** Configure las opciones de alerta antes de utilizar esta característica.

4. Haga clic en **Apply** y **OK**.

8.3.2 Crear una carpeta

GFI EventsManager le permite crear tantas carpetas recurrentes como sea necesario.

Para crear una carpeta:

1. En la ficha **Reporting > Reports**, haga clic con el botón secundario en una raíz o subcarpeta y seleccione **Create Folder**.

2. En la ficha **General**, especifique el nombre y una descripción (opcional) para el nuevo grupo.

3. Haga clic en la ficha **Schedule** y configure los parámetros de programación requeridos.

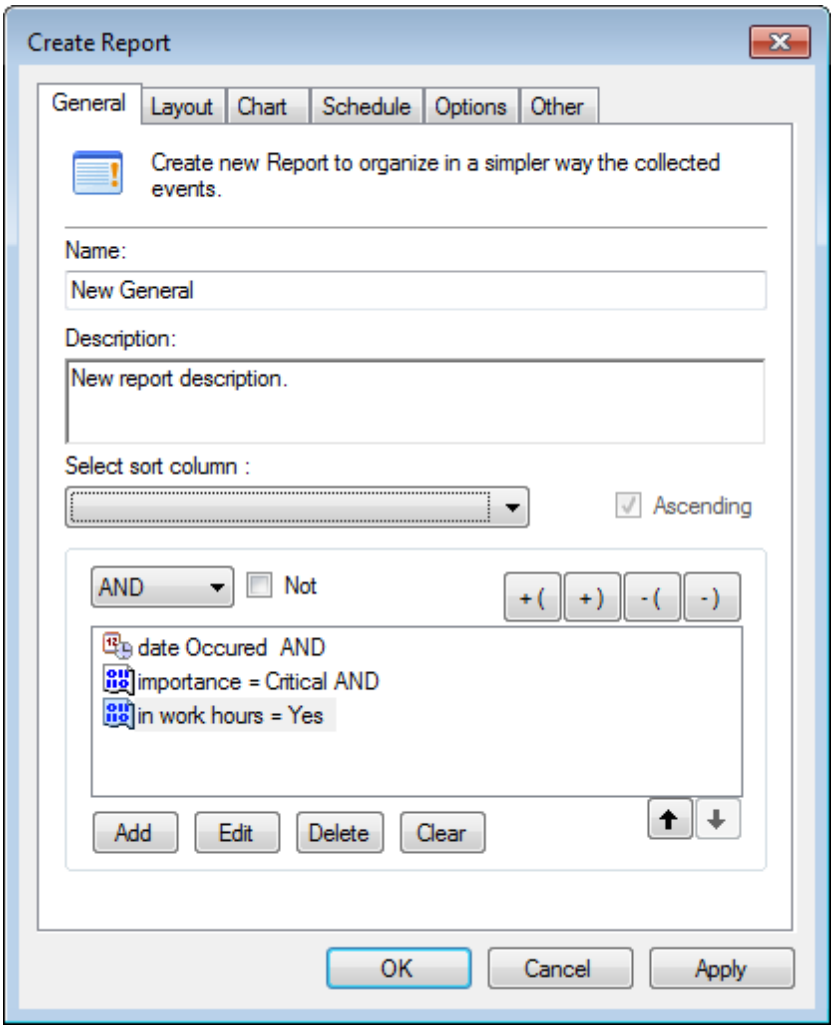
4. Haga clic en **Apply** y **OK**.

8.4 Crear un informe raíz

Los informes raíz se comportan de la misma manera que las carpetas raíz. Estos se crean en el nivel superior y pueden contener una serie de informes secundarios. Por ejemplo, usted puede crear un informe raíz que se genere de forma mensual y que contenga información acerca de inicios de sesión exitosos, conexiones fallidas y bloqueos de cuentas. Sus informes secundarios solamente contendrían información sobre partes específicas del informe raíz, como únicamente los inicios de sesión fallidos, generados a diario.

Para crear un informe raíz:

1. En la ficha **Reporting > Common Tasks**, haga clic en **Create Root Report**.



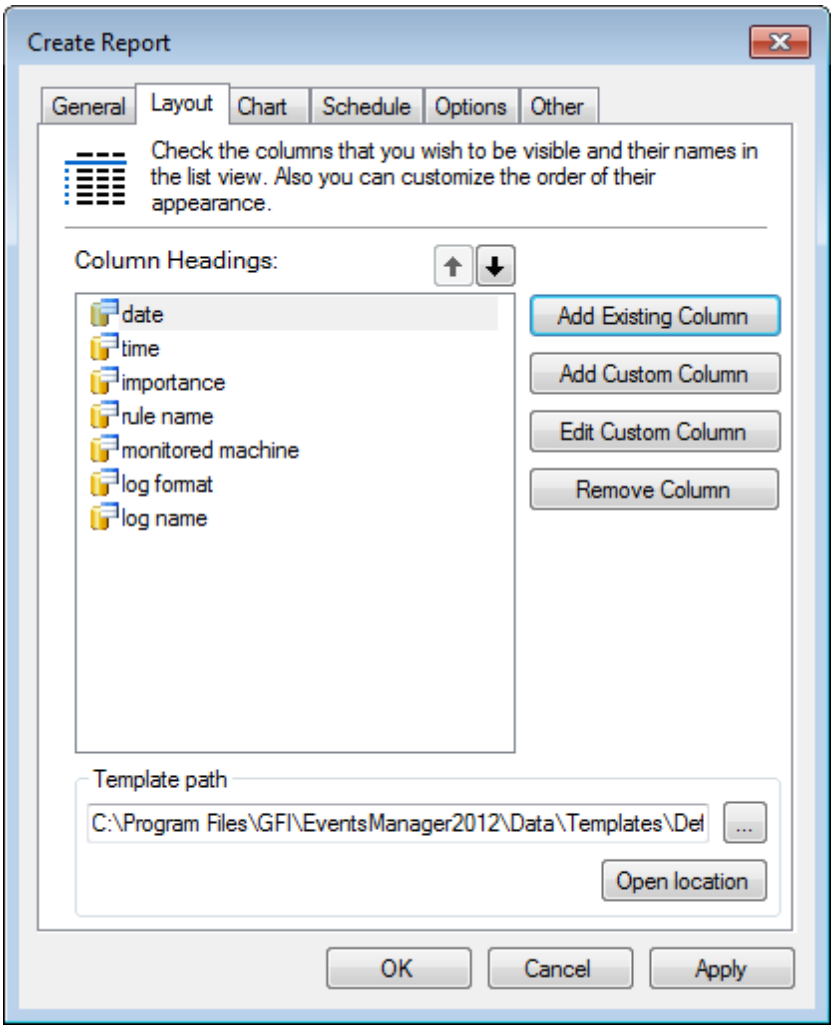
Captura de pantalla 104: Crear un informe raíz

2. En la ficha **General**, especifique un nombre y una descripción (opcional) para el nuevo informe raíz.

3. Haga clic en **Add** para seleccionar un campo en el que desea basar la condición de consulta. Para el campo seleccionado, especifique **Field Operator** y **Field Value**. Haga clic en **OK** para aceptar.

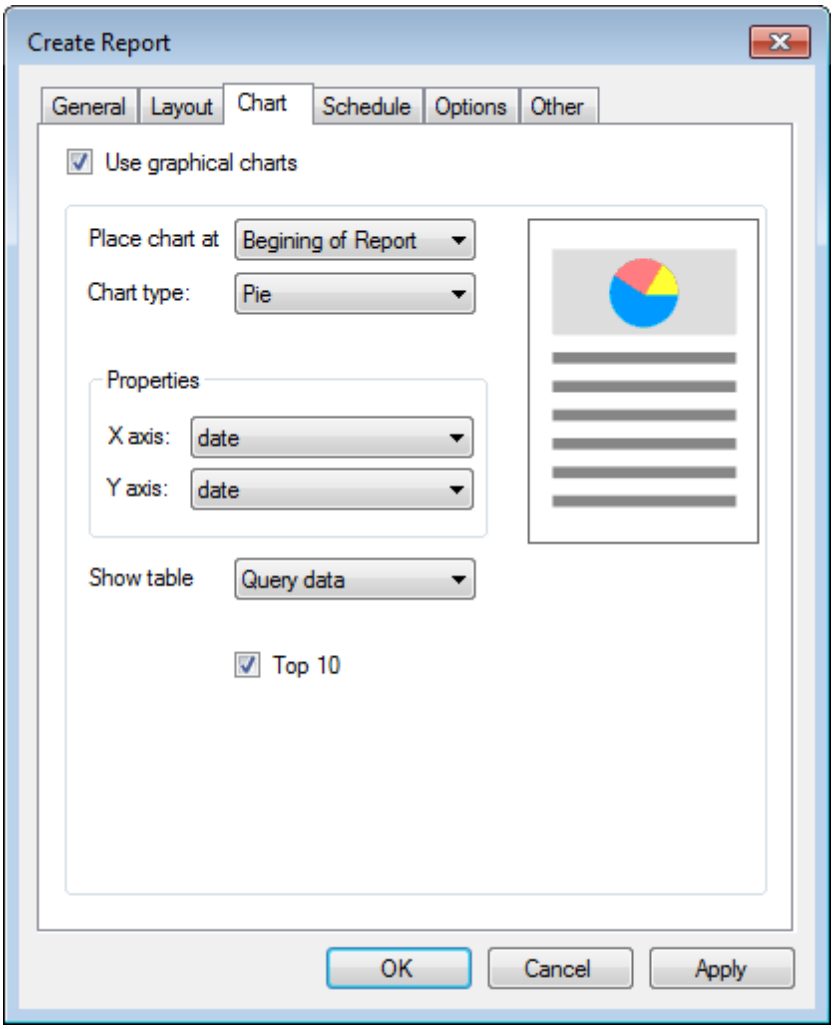
Nota

Repita este paso hasta seleccionar todos los campos obligatorios. Para obtener más información, consulte Diseñar restricciones de consulta.



Captura de pantalla 105: Configurar opciones de diseño del nuevo informe raíz

4. Haga clic en la ficha **Layout** y agregue los encabezados de columna que desea mostrar en el informe. Si tiene una plantilla de informe guardada, haga clic en **Open location** para buscar y cargar su plantilla. Para obtener más información, consulte Definir encabezados de columna.



Captura de pantalla 106: Insertar un gráfico en un nuevo informe raíz

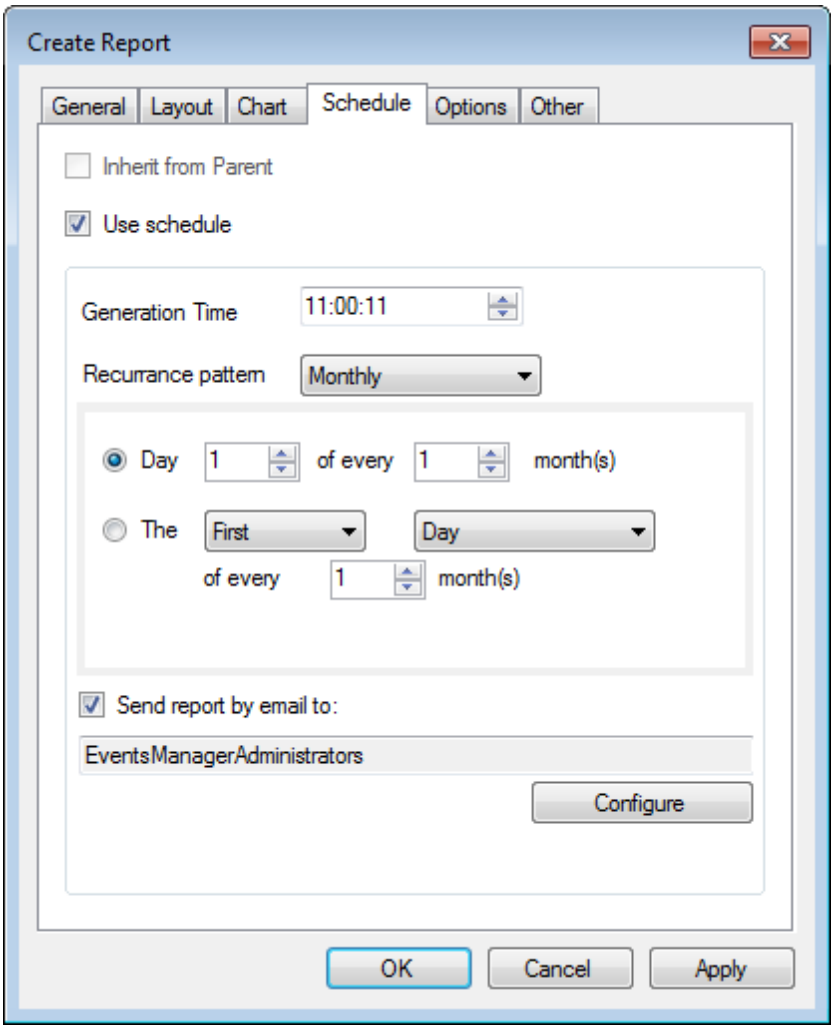
5. (Opcional) Haga clic en la ficha **Chart** y seleccione **Use graphical charts** para incluir gráficos en el informe.

6. En el menú desplegable **Place chart at**, especifique la ubicación del gráfico. Seleccione una de las siguientes opciones:

- Beginning of Report para colocarlo al inicio del informe
- End of Report para colocarlo al final del informe

7. En **Properties > X axis** y **Y axis**, configure las propiedades de los ejes X e Y. Es decir, seleccione los datos representados en el gráfico.

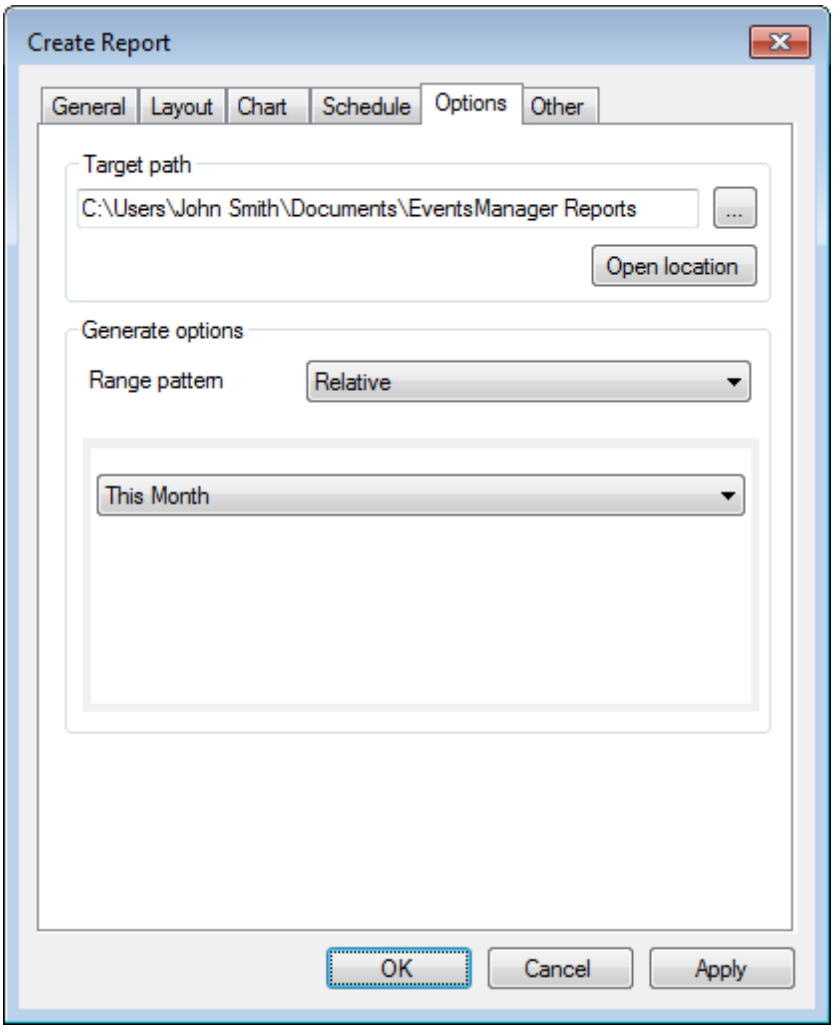
8. Seleccione **Top 10** para ver los primeros 10 registros únicamente.



Captura de pantalla 107: Configurar programación de generación de informes

9. (Opcional) Haga clic en la ficha **Schedule** y configure los parámetros de programación.

10. Seleccione **Send report by email to** y haga clic en **Configure** para seleccionar los destinatarios del informe.



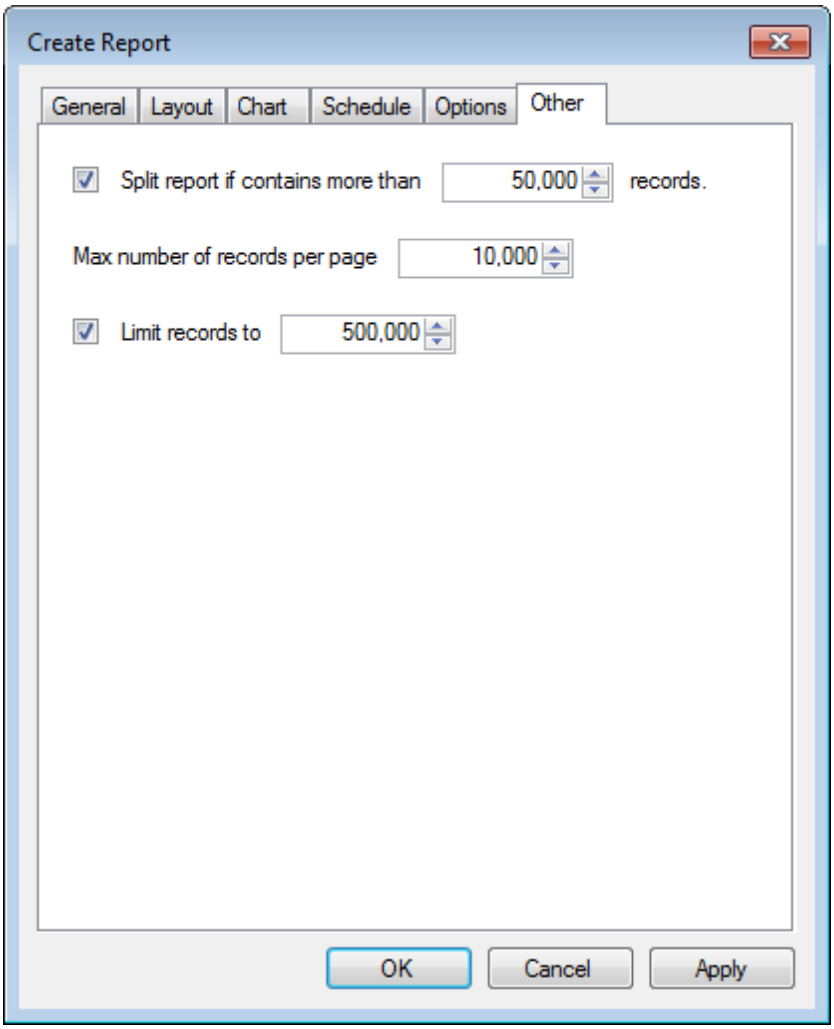
Captura de pantalla 108: Opciones para crear nuevo informe

11. Haga clic en la ficha **Options** y especifique la ruta en la que se debe generar el informe en el área **Target path**.

12. En el menú desplegable **Range pattern**, seleccione las opciones que se describen en la siguiente tabla:

Tabla 49: Opciones de patrón de rango

Patrón	Descripción
All Time	Seleccione **All Time** para generar el informe en función de la información de todos los registros relacionados.
Relative	Permite generar el informe en función de los siguientes eventos: » Today, para el día de hoy » Yesterday, para ayer » Last 7 Days, para los últimos 7 días » This Month, para este mes » Last Month, para el último mes
Día	Especifique un solo día en el que desea basar el informe.
Month	Especifique el mes y el año en el que desea basar el informe.
Date Range	Especifique una fecha **From** y **To** para basar el informe en eventos recopilados en un período específico de tiempo.



Captura de pantalla 109: Configuración de límite de registro

13. Haga clic en la ficha **Other** para configurar los límites de registro del informe. Las opciones disponibles se describen en la siguiente tabla:

Tabla 50: Configuración de registro del informe

Opción	Descripción
Split report if it contains more than {X} records	Marque la casilla de comprobación para habilitar el límite de registro por informe. GFI EventsManager crea automáticamente un nuevo informe para cada número de registros especificado. Por ejemplo: si escribe 50, 000, y el informe contiene 150, 000 registros, GFI EventsManager genera tres informes.
Max number of records per page	Especifique el número de registros que se muestran en una sola página.
Limit records to	Especifique el número máximo de registros que se incluyen en el informe. Se ignoran los registros que superan el límite.

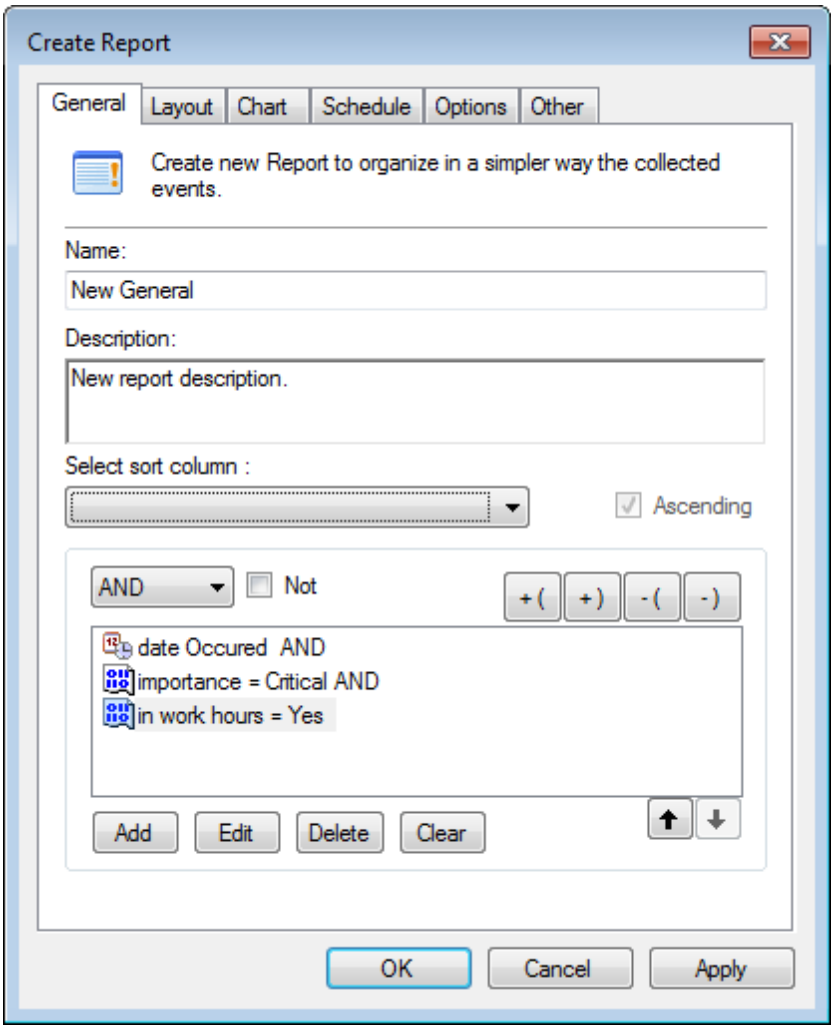
14. Haga clic en **Apply** y **OK**.

8.5 Crear informes personalizados

La creación de informes personalizados requiere planificación mientras se configuran las condiciones. Las condiciones se establecen para determinar lo que se filtra y se presenta en el informe. Si no se configuran las condiciones correctamente, se genera ruido no deseado e información inexacta.

Para crear un nuevo informe personalizado:

1. En la ficha **Reporting > Reports**, haga clic con el botón secundario en una carpeta/carpeta raíz/informe raíz y seleccione **Create Report**.

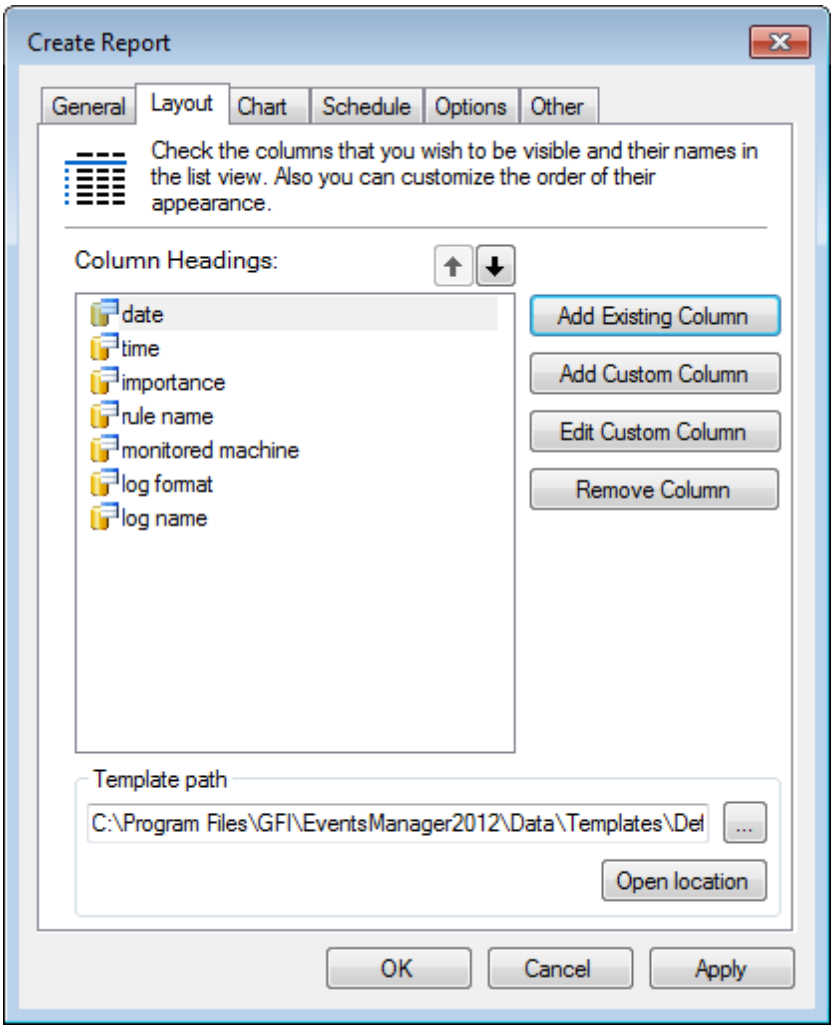


Captura de pantalla 110: Crear un informe raíz

2. En la ficha **General**, especifique un nombre y una descripción (opcional) para el nuevo informe raíz.

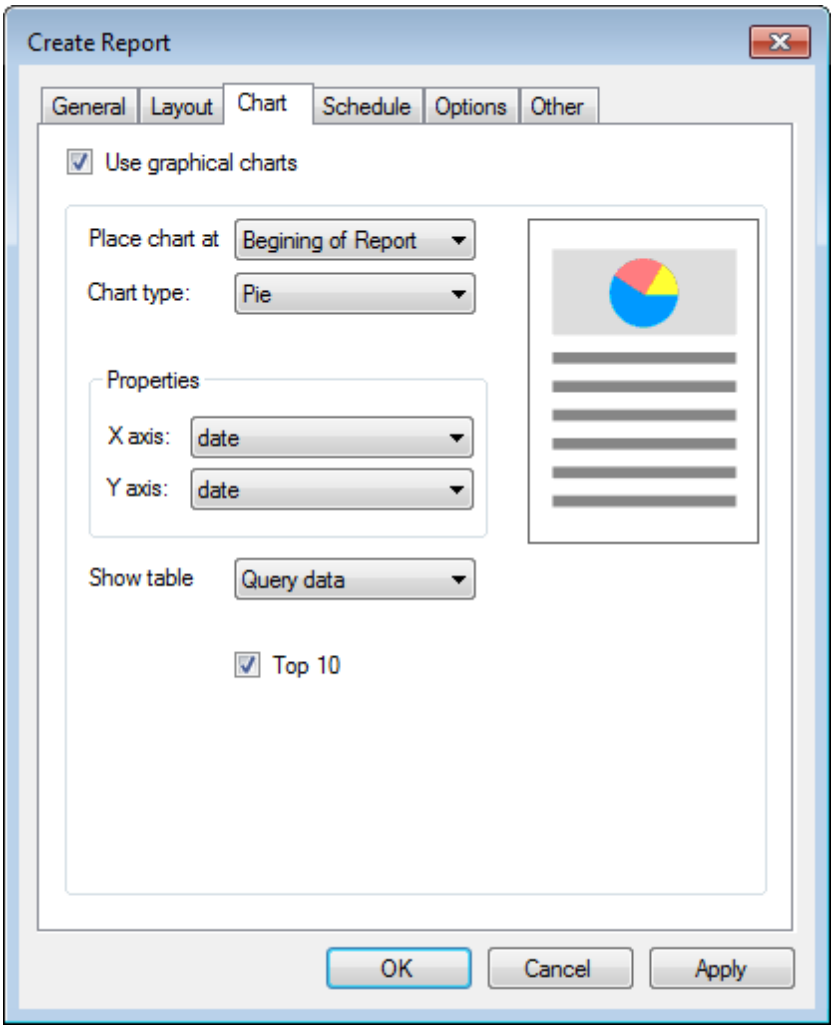
3. Haga clic en **Add** para seleccionar un campo en el que desea basar la condición de consulta. Para el campo seleccionado, especifique **Field Operator** y **Field Value**. Haga clic en **OK** para aceptar.

> **Nota**
>
> Repita este paso hasta seleccionar todos los campos obligatorios. Para obtener más información, consulte Diseñar restricciones de consulta.



Captura de pantalla 111: Configurar opciones de diseño del nuevo informe raíz

4. Haga clic en la ficha **Layout** y agregue los encabezados de columna que desea mostrar en el informe. Si tiene una plantilla de informe guardada, haga clic en **Open location** para buscar y cargar su plantilla. Para obtener más información, consulte Definir encabezados de columna.



Captura de pantalla 112: Insertar un gráfico en un nuevo informe raíz

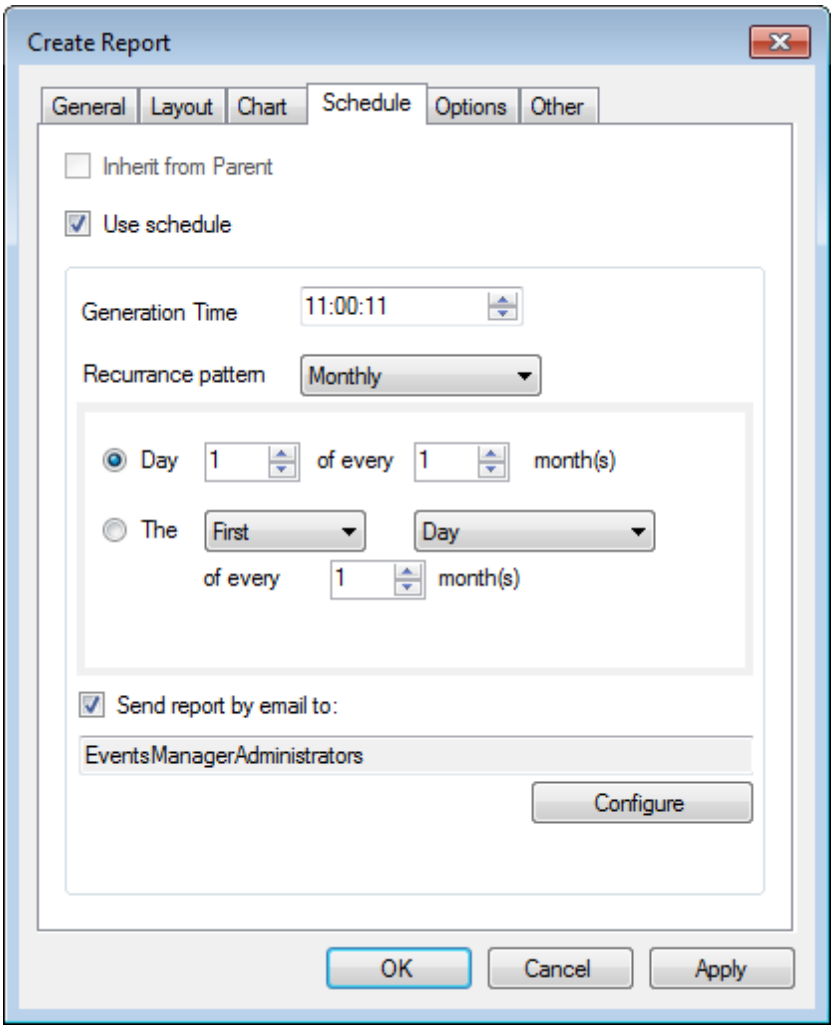
5. (Opcional) Haga clic en la ficha **Chart** y seleccione **Use graphical charts** para incluir gráficos en el informe.

6. En el menú desplegable **Place chart at**, especifique la ubicación del gráfico. Seleccione una de las siguientes opciones:

- Beginning of Report para colocarlo al inicio del informe
- End of Report para colocarlo al final del informe

7. En **Properties > X axis** y **Y axis**, configure las propiedades de los ejes X e Y. Es decir, seleccione los datos representados en el gráfico.

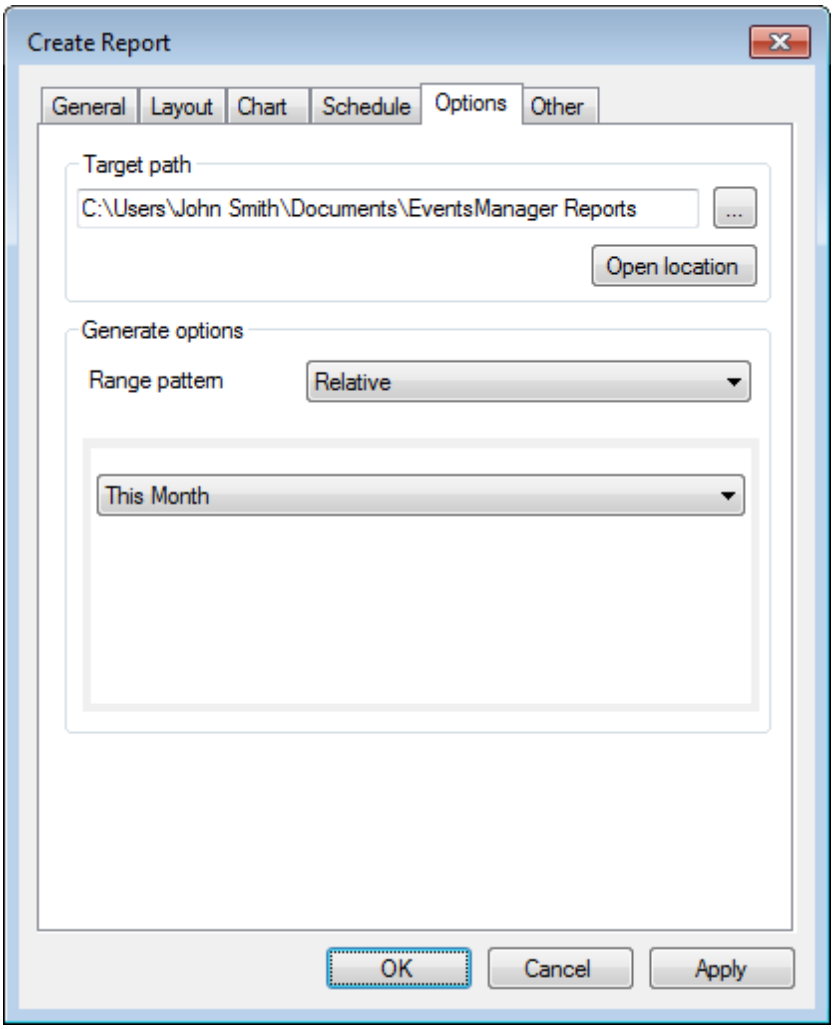
8. Seleccione **Top 10** para ver los primeros 10 registros únicamente.



Captura de pantalla 113: Configurar programación de generación de informes

9. (Opcional) Haga clic en la ficha **Schedule** y configure los parámetros de programación.

10. Seleccione **Send report by email to** y haga clic en **Configure** para seleccionar los destinatarios del informe.



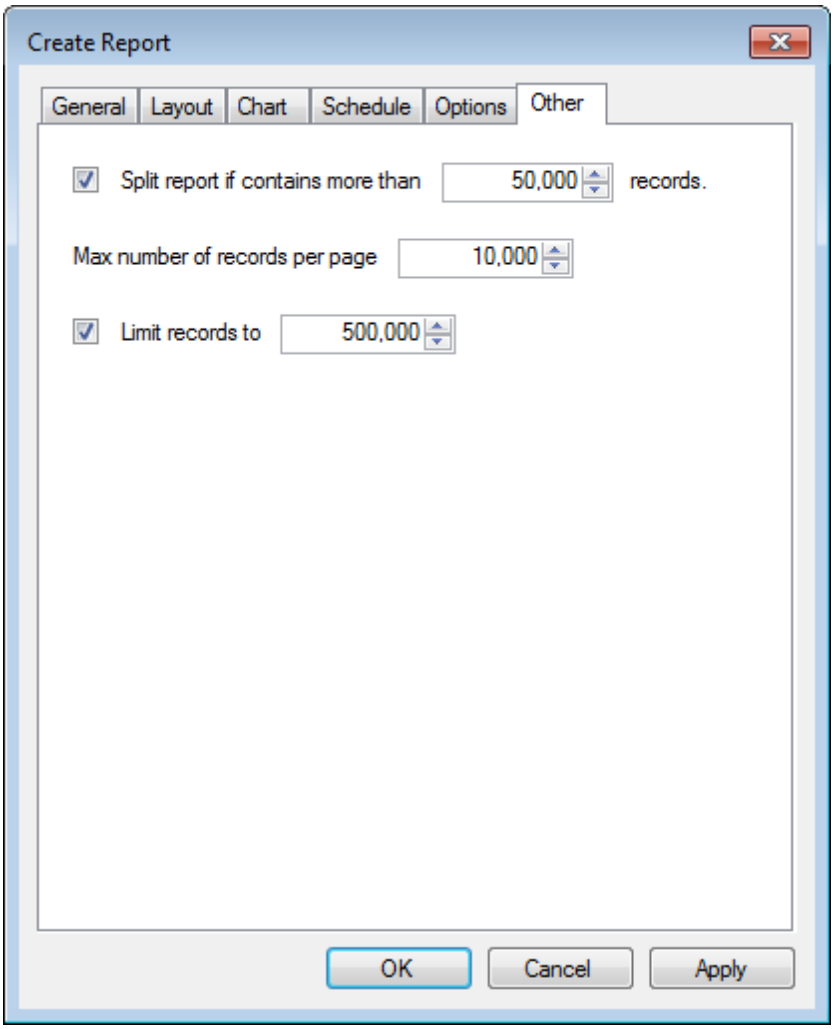
Captura de pantalla 114: Opciones para crear nuevo informe

11. Haga clic en la ficha **Options** y especifique la ruta en la que se debe generar el informe en el área **Target path**.

12. En el menú desplegable **Range pattern**, seleccione las opciones que se describen en la siguiente tabla:

Tabla 51: Opciones de patrón de rango

Patrón	Descripción
All Time	Seleccione **All Time** para generar el informe en función de la información de todos los registros relacionados.
Relative	Permite generar el informe en función de los siguientes eventos: » Today, para el día de hoy » Yesterday, para ayer » Last 7 Days, para los últimos 7 días » This Month, para este mes » Last Month, para el último mes
Día	Especifique un solo día en el que desea basar el informe.
Month	Especifique el mes y el año en el que desea basar el informe.
Date Range	Especifique una fecha **From** y **To** para basar el informe en eventos recopilados en un período específico de tiempo.



Captura de pantalla 115: Configuración de límite de registro

13. Haga clic en la ficha **Other** para configurar los límites de registro del informe. Las opciones disponibles se describen en la siguiente tabla:

Tabla 52: Configuración de registro del informe

Opción	Descripción
Split report if it contains more than {X} records	Marque la casilla de comprobación para habilitar el límite de registro por informe. GFI EventsManager crea automáticamente un nuevo informe para cada número de registros especificado. Por ejemplo: si escribe 50, 000, y el informe contiene 150, 000 registros, GFI EventsManager genera tres informes.
Max number of records per page	Especifique el número de registros que se muestran en una sola página.
Limit records to	Especifique el número máximo de registros que se incluyen en el informe. Se ignoran los registros que superan el límite.

14. Haga clic en **Apply** y **OK**.

8.6 Generar informes

GFI EventsManager le permite generar una serie de informes diferentes, que contienen información sobre los parámetros de configuración, la actividad de la red y la actividad de GFI EventsManager.

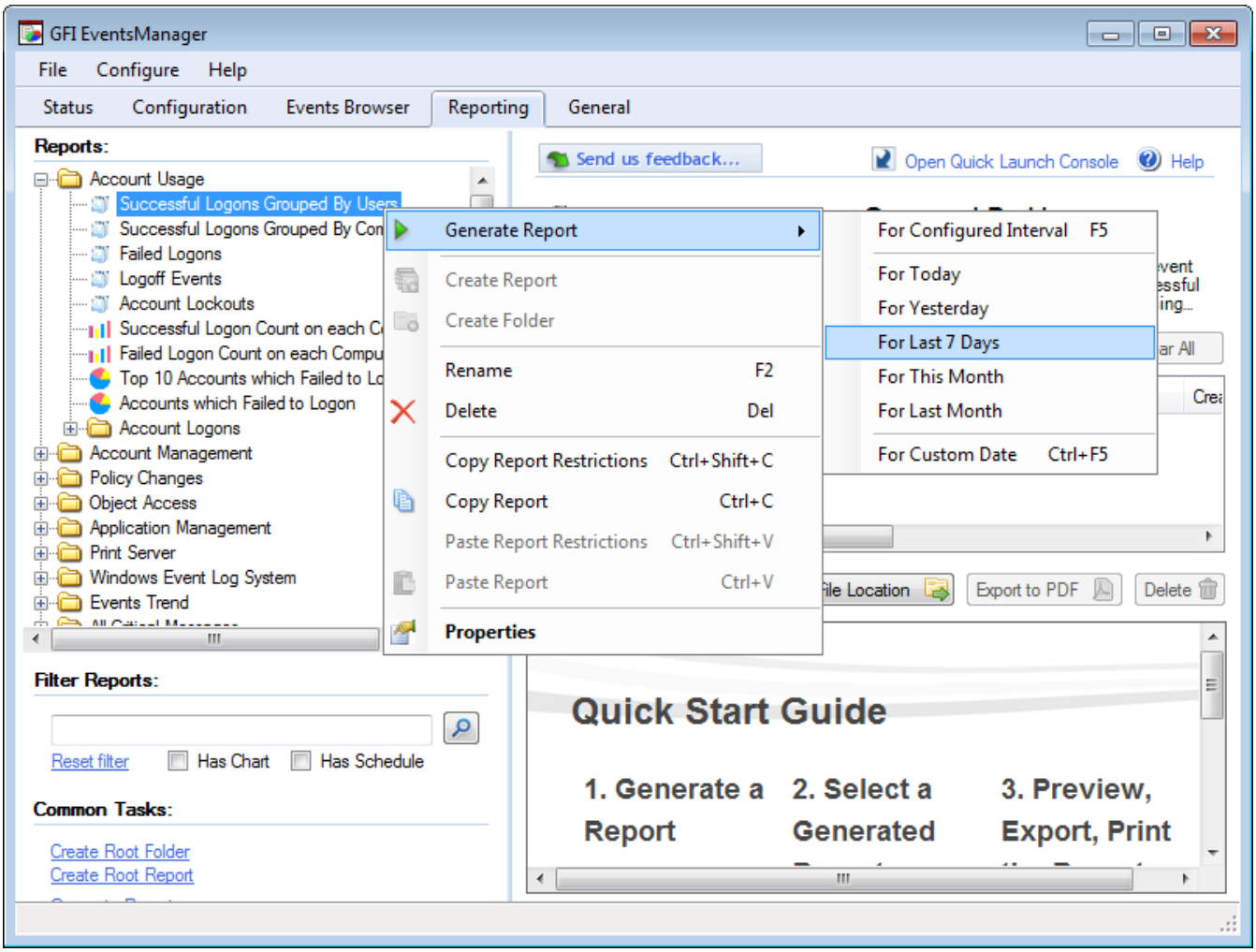
Esta sección contiene información acerca de:

- Generar un informe
- Generar informes de resumen diario
- Generar informes de configuración
- Generar informes de reglas
- Generar informes del historial operativo
- Generar informes de descripción general de actividad

8.6.1 Generar un informe

Para generar un informe:

1. En la ficha **Reporting > Reports**, haga clic con el botón secundario en un informe y seleccione **Generate Report**.

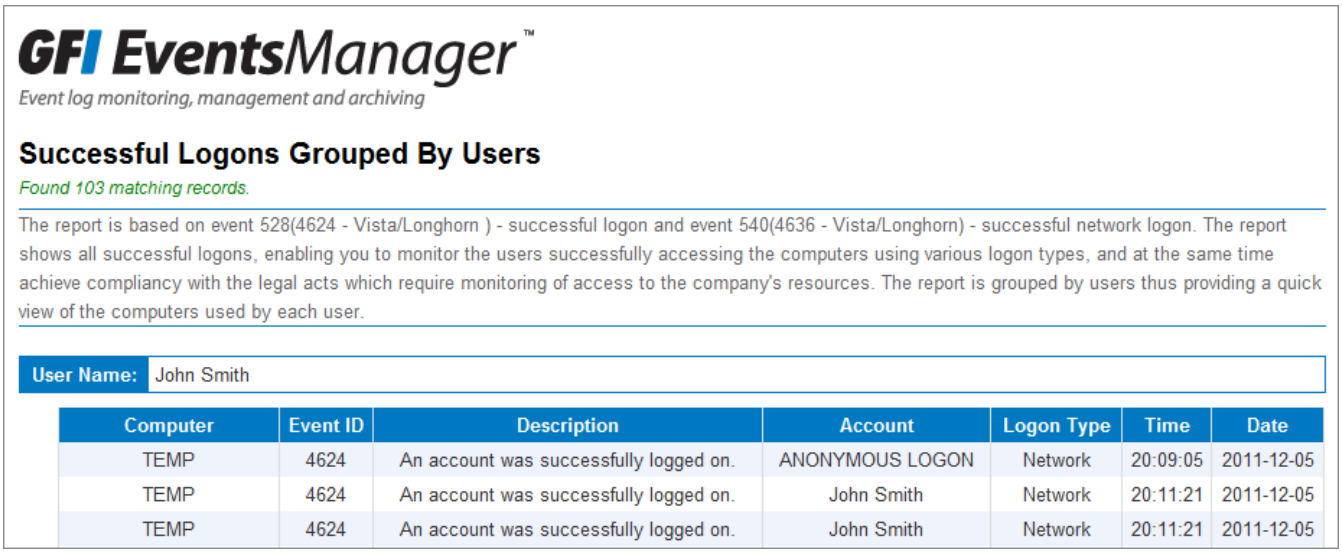


Captura de pantalla 116: Generar un informe

2. Espere hasta que el informe se genere y vea los resultados en la sección **Preview Report**.

Nota

Los informes también se pueden generar mediante la selección de un informe de la lista y haciendo clic en **Generate Report** en la parte superior de la página de informe.



GFI EventsManager™

Event log monitoring, management and archiving

Successful Logons Grouped By Users

Found 103 matching records.

The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.

User Name: John Smith

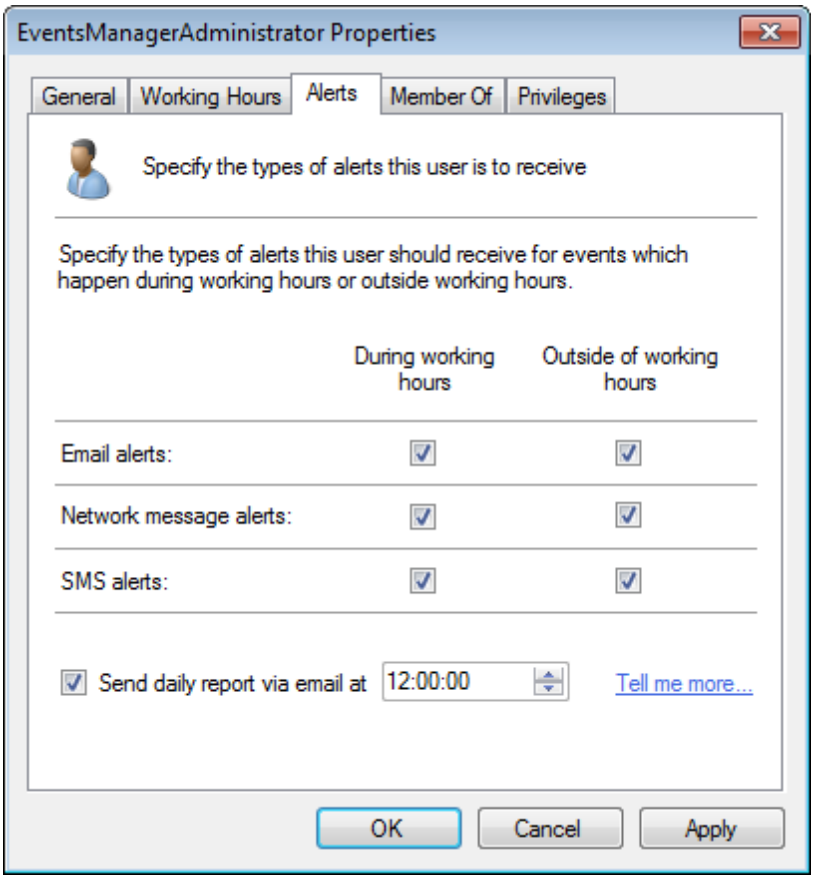
Computer	Event ID	Description	Account	Logon Type	Time	Date
TEMP	4624	An account was successfully logged on.	ANONYMOUS LOGON	Network	20:09:05	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05

Captura de pantalla 117: Muestra de informe

8.6.2 Generar informes de resumen diarios

GFI EventsManager puede configurarse para enviar un informe de resumen por correo electrónico todos los días. El informe contiene un resumen de los eventos más importantes recopilados y procesados durante las últimas 24 horas. Para configurar un usuario y enviarle el resumen diario por correo electrónico:

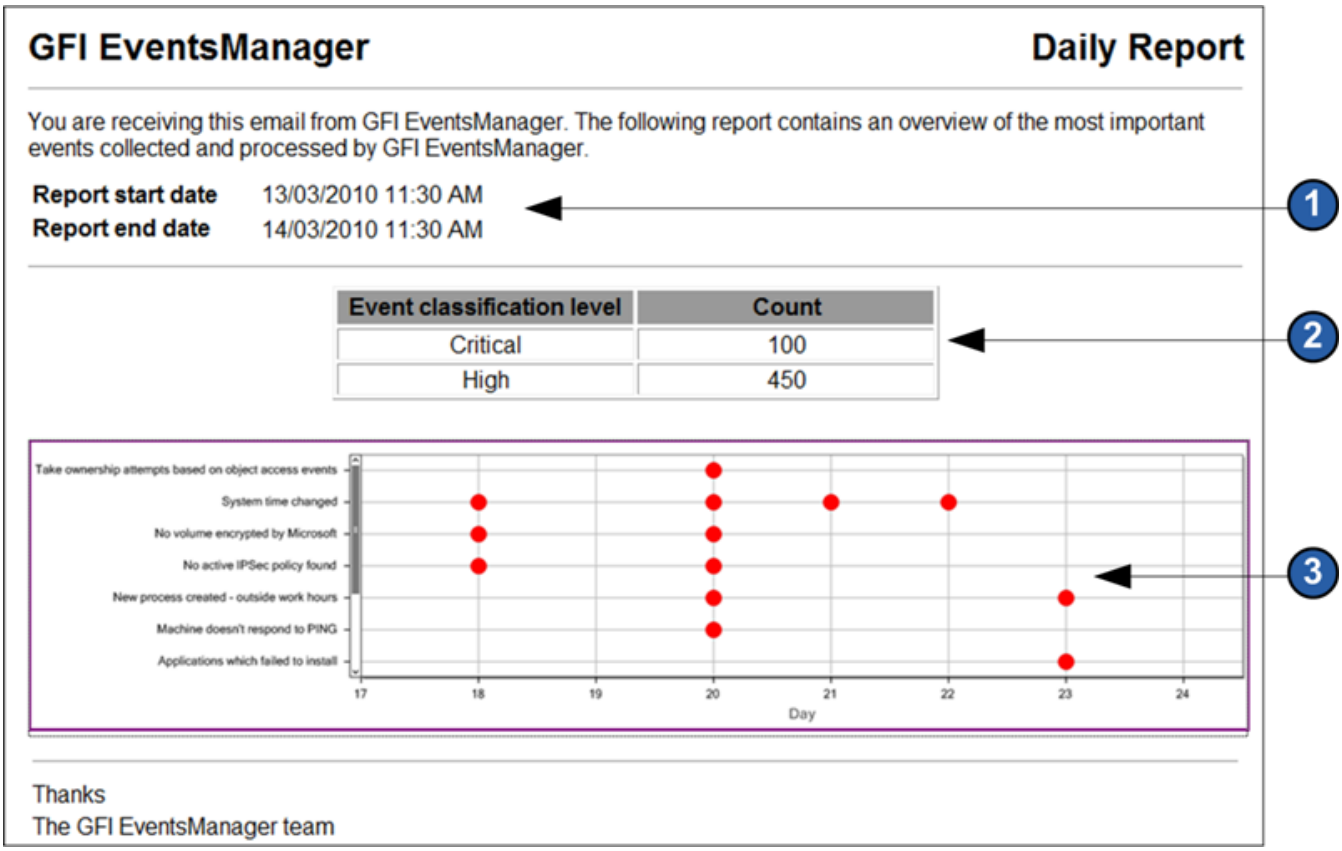
1. En la ficha **Configuration > Options**. Expanda **Users and Groups** y seleccione **Users**.
2. Haga clic con el botón secundario en un usuario en el panel derecho y seleccione **Properties**.
3. En la ficha **General**, asegúrese de especificar una dirección de correo electrónico válida.
4. En la ficha **Alerts**, seleccione **Send daily report via email**.



Captura de pantalla 118: Configuración de resumen diario por correo electrónico

5. Configure el momento en que se envía el resumen diario por correo electrónico.

6. Haga clic en **Apply** y **OK**.



Captura de pantalla 119: Resumen diario por correo electrónico

Tabla 53: Descripción del resumen diario por correo electrónico

Sección	Description
1	La fecha de inicio y fin del informe. El informe muestra los hechos más importantes recopilados por GFI EventsManager entre la fecha de inicio y fin.
2	El número de eventos de importancia crítica y alta recopilados en las últimas 24 horas.
3	En este gráfico, se ofrece información estadística acerca de los eventos de importancia crítica recopilados de todos los orígenes de eventos en las últimas 24 horas.

8.6.3 Generar informes de configuración

GFI EventsManager le permite generar informes de configuración en grupos de orígenes de eventos. La información proporcionada se describe a continuación:

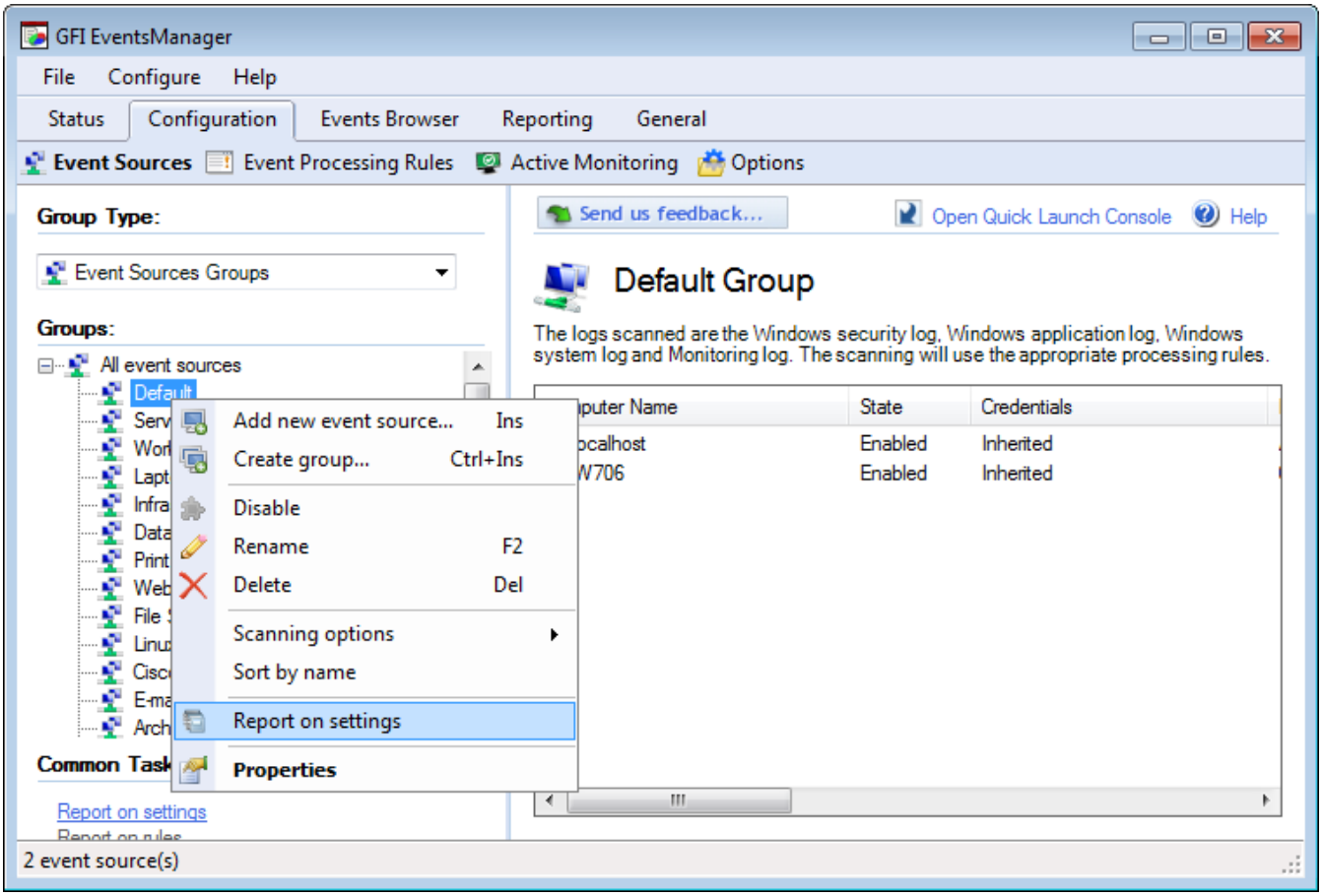
Tabla 54: Información de encabezado del informe de configuración

Encabezado	Descripción
Group name	El nombre del grupo en el que se basa el informe.
Computer name	Una lista de todos los orígenes de eventos en el grupo seleccionado.
Scan intervals	Intervalo de análisis para cada origen de evento en el grupo seleccionado; se muestra en **días: horas: minutos: segundos**.

Encabezado	Descripción
Rules folder	Proporciona una lista de categorías de reglas aplicadas para el grupo seleccionado, tales como: » Reducción de ruido » Seguridad » Estado del sistema » Requisitos de PCI DSS
Rule sets	Una lista granular de las reglas aplicadas al grupo seleccionado.

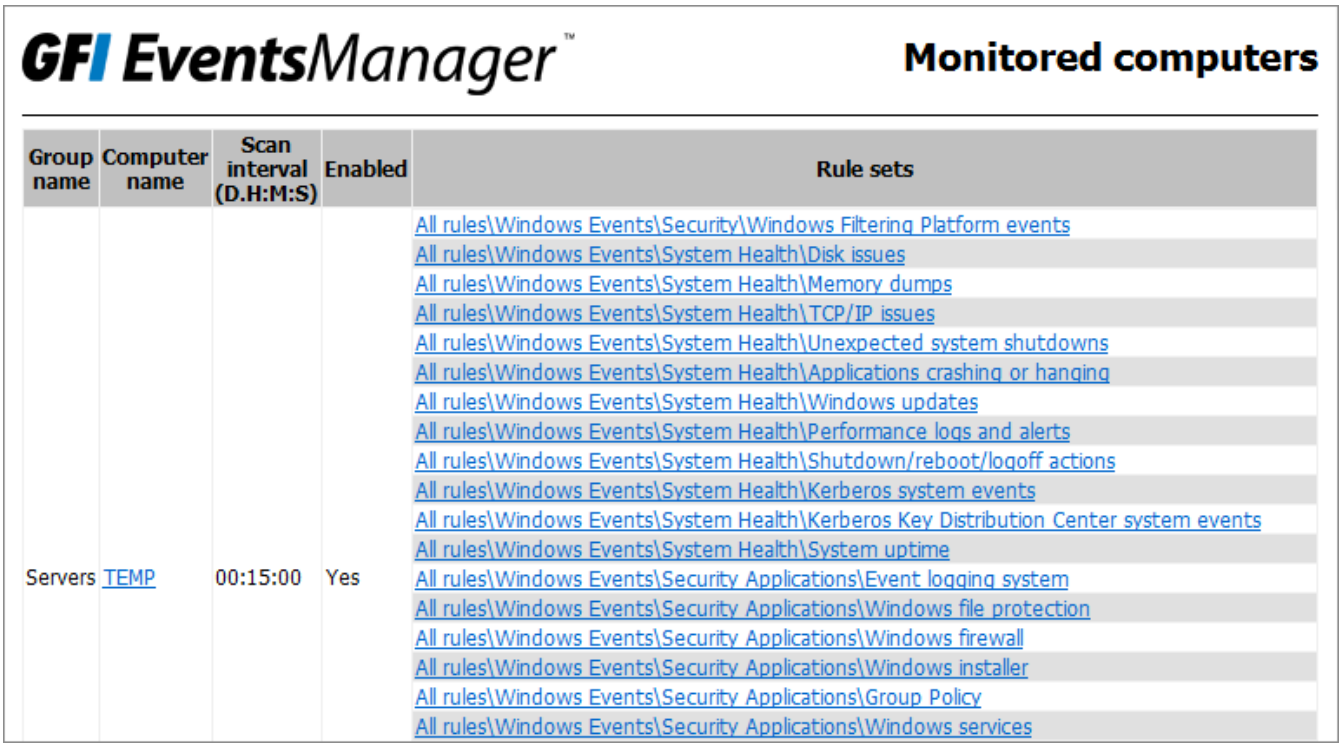
Para generar un informe de configuración:

1. Haga clic en la ficha **Configuration > Event Sources**.



Captura de pantalla 120: Generar informe de configuración

2. Haga clic con el botón secundario en un grupo de orígenes de eventos y seleccione **Report on settings**.



GFI EventsManager™ **Monitored computers**

Group name	Computer name	Scan interval (D.H:M:S)	Enabled	Rule sets
Servers	TEMP	00:15:00	Yes	All rules\Windows Events\Security\Windows Filtering Platform events All rules\Windows Events\System Health\Disk issues All rules\Windows Events\System Health\Memory dumps All rules\Windows Events\System Health\TCP/IP issues All rules\Windows Events\System Health\Unexpected system shutdowns All rules\Windows Events\System Health\Applications crashing or hanging All rules\Windows Events\System Health\Windows updates All rules\Windows Events\System Health\Performance logs and alerts All rules\Windows Events\System Health\Shutdown/reboot/logoff actions All rules\Windows Events\System Health\Kerberos system events All rules\Windows Events\System Health\Kerberos Key Distribution Center system events All rules\Windows Events\System Health\System uptime All rules\Windows Events\Security Applications\Event logging system All rules\Windows Events\Security Applications\Windows file protection All rules\Windows Events\Security Applications\Windows firewall All rules\Windows Events\Security Applications\Windows installer All rules\Windows Events\Security Applications\Group Policy All rules\Windows Events\Security Applications\Windows services

Captura de pantalla 121: Muestra de informe de configuración

8.6.4 Generar informes de reglas

Los informes de reglas proporcionan una vista detallada de las reglas aplicadas a los orígenes de eventos. La información proporcionada en los informes de reglas se describe a continuación:

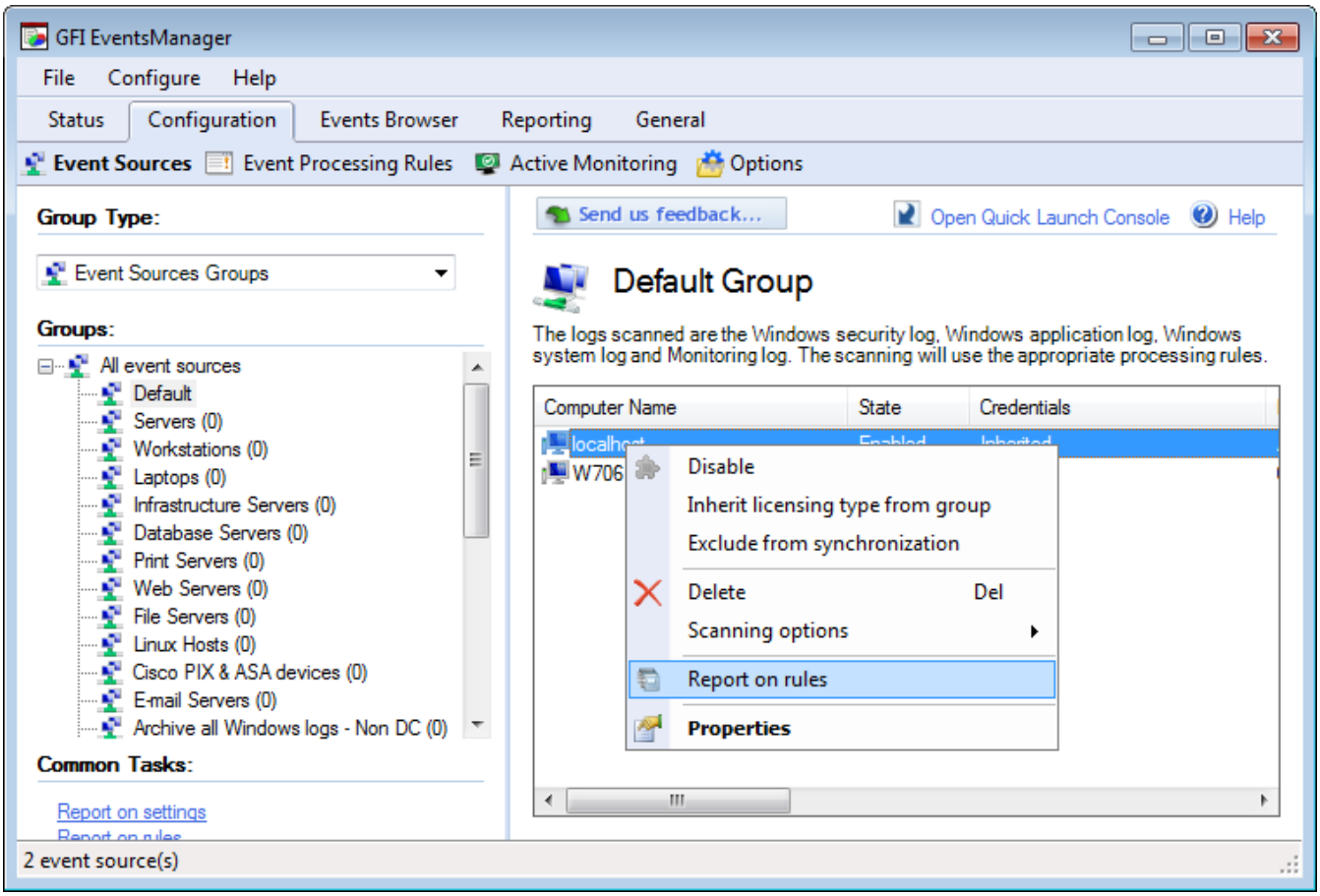
Tabla 55: Información de encabezado del informe de reglas

Encabezado	Description
Rule name	Nombre de la norma aplicada.
Importance	El nivel de importancia clasificada del registro de eventos recopilados, como: » Crítica » Alta » Media » Baja » Ruido
Logfile monitored	Proporciona el nombre de la categoría del registro de eventos recopilados, como: » Seguridad » Estado del sistema » Aplicación » Sistema
Conditions	Las condiciones de procesamiento de la regla seleccionada. Esto incluye: » ID de evento » Origen » Categoría » Usuario » Tipo » Avanzadas

Encabezado	Description
Actions	Describe las acciones realizadas cuando se procesa el evento, incluso: » Configuración de almacenamiento » Correo a configuración » Configuración del umbral

Para generar un informe de reglas:

1. Haga clic en la ficha **Configuration > Event Sources**.



Captura de pantalla 122: Generar informe de configuración

2. Haga clic en un origen de eventos y seleccione **Report on rules**.

8.6.5 Generar informes del historial operativo

El historial operativo de GFI EventsManager se puede exportar para su posterior análisis y para fines de almacenamiento. Los mensajes del historial operativo proporcionan a los administradores la información que se describe a continuación:

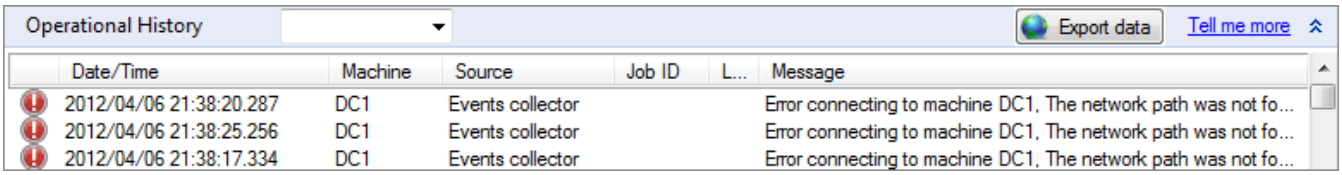
Tabla 56: Descripción del informe del historial operativo

Date/Time	La fecha y la hora en que se generó el mensaje.
Machine	Origen de evento que generó el mensaje.
Source	Operación de origen que generó el mensaje. Entre otras, se incluyen: » **EvtCollector**: mensaje generado al recopilar registros de eventos. » **SNMP TrapsServer**: mensaje generado durante la recopilación de capturas SNMP. » **EnetrpriseMaintenance**: mensaje generado durante las tareas de mantenimiento de la base de datos.

Job ID	Un ID interno asociado con la tarea.
Log file/name	El tipo de registros recopilados. Entre otros: Aplicación Seguridad Registros generados por otras aplicaciones, tales como GFI LanGuard y GFI EndPointSecurity.
Message	El mensaje real generado durante la ejecución de la tarea.

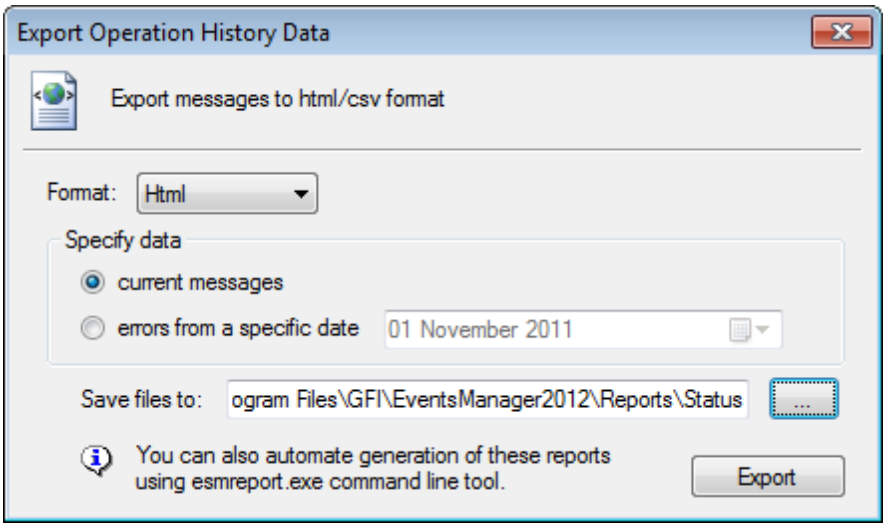
Para generar informes de historial operativo:

1. Haga clic en la ficha **Status > Job Activity**.


Operational History
Export data
Tell me more
Date/Time
Machine
Source
Job ID
L...
Message
2012/04/06 21:38:20.287 DC1 Events collector Error connecting to machine DC1, The network path was not fo...
2012/04/06 21:38:25.256 DC1 Events collector Error connecting to machine DC1, The network path was not fo...
2012/04/06 21:38:17.334 DC1 Events collector Error connecting to machine DC1, The network path was not fo...

Captura de pantalla 123: Informe del historial operativo

2. Haga clic en **Export data**.



Captura de pantalla 124: Cuadro de diálogo del historial operativo

3. Especifique las opciones que se describen a continuación y haga clic en **Export**.

Tabla 57: Opciones de exportación del historial operativo

Opción	Description
Format	Seleccione el formato de salida del informe. Los formatos disponibles son HTML y CSV.
Current messages	Permite exportar todos los mensajes que aparecen en la ficha Job Activity.
Errors from a specific date	Especifique una fecha y exporte todos los mensajes generados en esa fecha.
Save file to	Marque la casilla de verificación para especificar la ubicación de salida. Si no se marca, los informes se guardan en la ubicación predeterminada en el directorio de GFI EventsManager.

GFI EventsManager

Operational History for period: 2011-11-01

Date/Time	Type	Machine	Source	Job ID	Log file/name	Message
31/10/2011 18:41:03	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Start executing checks on machine 192.168.3.1..
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Executed 5 checks on machine 192.168.3.1
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	B3789E4A	Security	Start the collection on machine 192.168.3.1, log Security
31/10/2011 18:41:30	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.
31/10/2011 18:41:33	Information	192.168.3.1	EvtCollector	1017473C	Application	Start the collection on machine 192.168.3.1, log Application
31/10/2011 18:41:45	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.

Captura de pantalla 125: Muestra de informe del historial operativo

8.6.6 Generar informes de descripción general de actividades

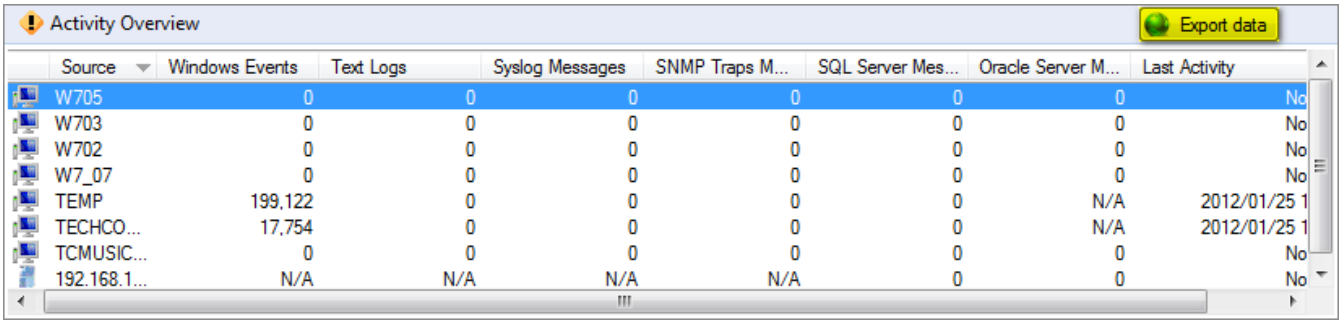
GFI EventsManager le permite exportar datos de descripción general de actividades. Los informes generales de actividad proporcionan la información que se describe a continuación:

Tabla 58: Encabezados de los informes generales de actividad

Encabezado	Description
Date/Time	La fecha y la hora en que se generó el mensaje.
Machine	Origen de evento que generó el mensaje.
Source	Operación de origen que generó el mensaje. Entre otras, se incluyen: » **EvtCollector**: mensaje generado al recopilar registros de eventos. » **SNMP Traps Server**: mensaje generado al recopilar mensajes de captura SNMP. » **EnetrpriseMaintenance**: mensaje generado durante las tareas de mantenimiento de la base de datos.
Job ID	Un ID interno asociado con la tarea.
Log file/name	El tipo de registros recopilados. Entre otros: » Aplicación » Seguridad » Registros generados por otras aplicaciones, como GFI LanGuard y GFI EndPointSecurity.
Message	El mensaje real generado durante la ejecución de la tarea.

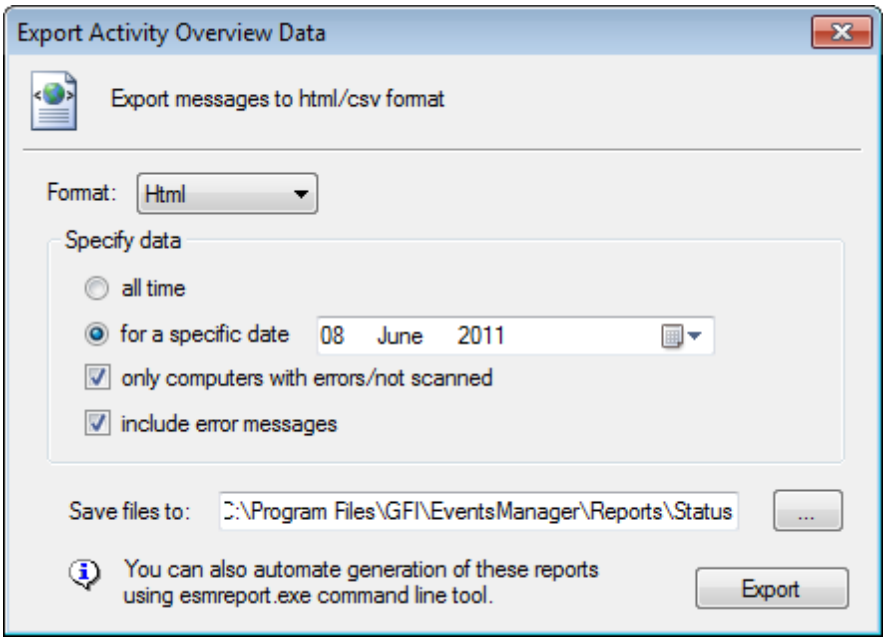
Para exportar la descripción general de actividades:

1. Haga clic en **Status > Statistics**.


Activity Overview
Export data
Source
Windows Events
Text Logs
Syslog Messages
SNMP Traps M...
SQL Server Mes...
Oracle Server M...
Last Activity
W705 0 0 0 0 0 0 No
W703 0 0 0 0 0 0 No
W702 0 0 0 0 0 0 No
W7_07 0 0 0 0 0 0 No
TEMP 199,122 0 0 0 0 N/A 2012/01/25 1
TECHCO... 17,754 0 0 0 0 N/A 2012/01/25 1
TCMUSIC... 0 0 0 0 0 0 No
192.168.1... N/A N/A N/A N/A 0 0 No

Captura de pantalla 126: Descripción general de la actividad: Botón para exportar

2. Haga clic en **Export data**.



Captura de pantalla 127: Cuadro de diálogo de descripción general de actividades

3. Configure las opciones descritas y haga clic en **Export**.

Tabla 59: Opciones de exportación del historial operativo

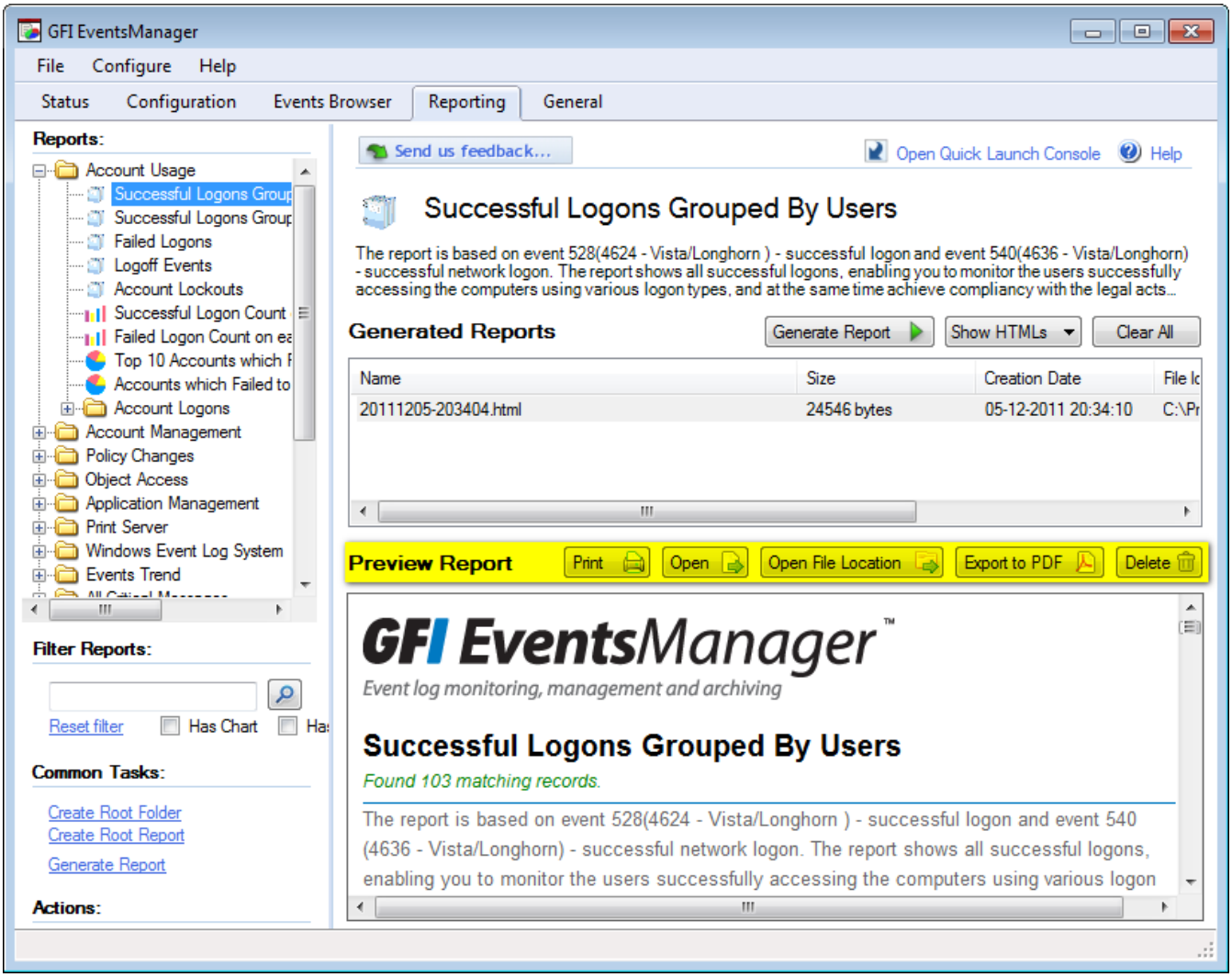
Opción	Description
Format	El formato de salida del informe. Los formatos disponibles son HTML y CSV.
All time	Exportar todos los mensajes que se muestran en la descripción general de actividad.
From a specific date	Especifique una fecha para exportar todos los mensajes generados en esa fecha.
Only computers with errors/not scanned	Permite exportar solamente los datos de los equipos con problemas en el análisis.
Include error messages	Seleccione esta opción para incluir el mensaje de error generado.
Save files to	Muestra la ubicación de exportación predeterminada.

GFI EventsManager™ **Activity Overview for period: 2012/01/25**

Source	Windows Events	Text Logs Events	Syslog Messages	SNMP Traps Messages	SQL Server Messages	Oracle Server Messages	Last Activity
TCMUSICSERVER	0	N/A	N/A	N/A	N/A	N/A	No Activity
TECHCOMSERVTWO	23753	N/A	N/A	N/A	N/A	N/A	2012/01/25 18:08:00.933
TEMP	196799	N/A	N/A	N/A	N/A	N/A	2012/01/25 17:55:47.542
W7_07	0	N/A	N/A	N/A	N/A	N/A	No Activity
W702	0	N/A	N/A	N/A	N/A	N/A	No Activity
W703	0	N/A	N/A	N/A	N/A	N/A	No Activity
W705	0	N/A	N/A	N/A	N/A	N/A	No Activity
192.168.11.11	N/A	N/A	N/A	N/A	N/A	0	No Activity

Captura de pantalla 128: Muestra de informe de descripción general de actividad

8.7 Analizar informes



Captura de pantalla 129: Analizar informes

El sistema de información de GFI EventsManager cuenta con herramientas específicas para ayudarlo a analizar y exportar informes. Una vez que se genera un informe, selecciónelo en la lista de informes generados y utilice los controles comunes que ayudan a ejecutar comandos comunes de análisis de informes. A continuación, se describen las herramientas disponibles:

Tabla 60: Analizar informes: Herramientas

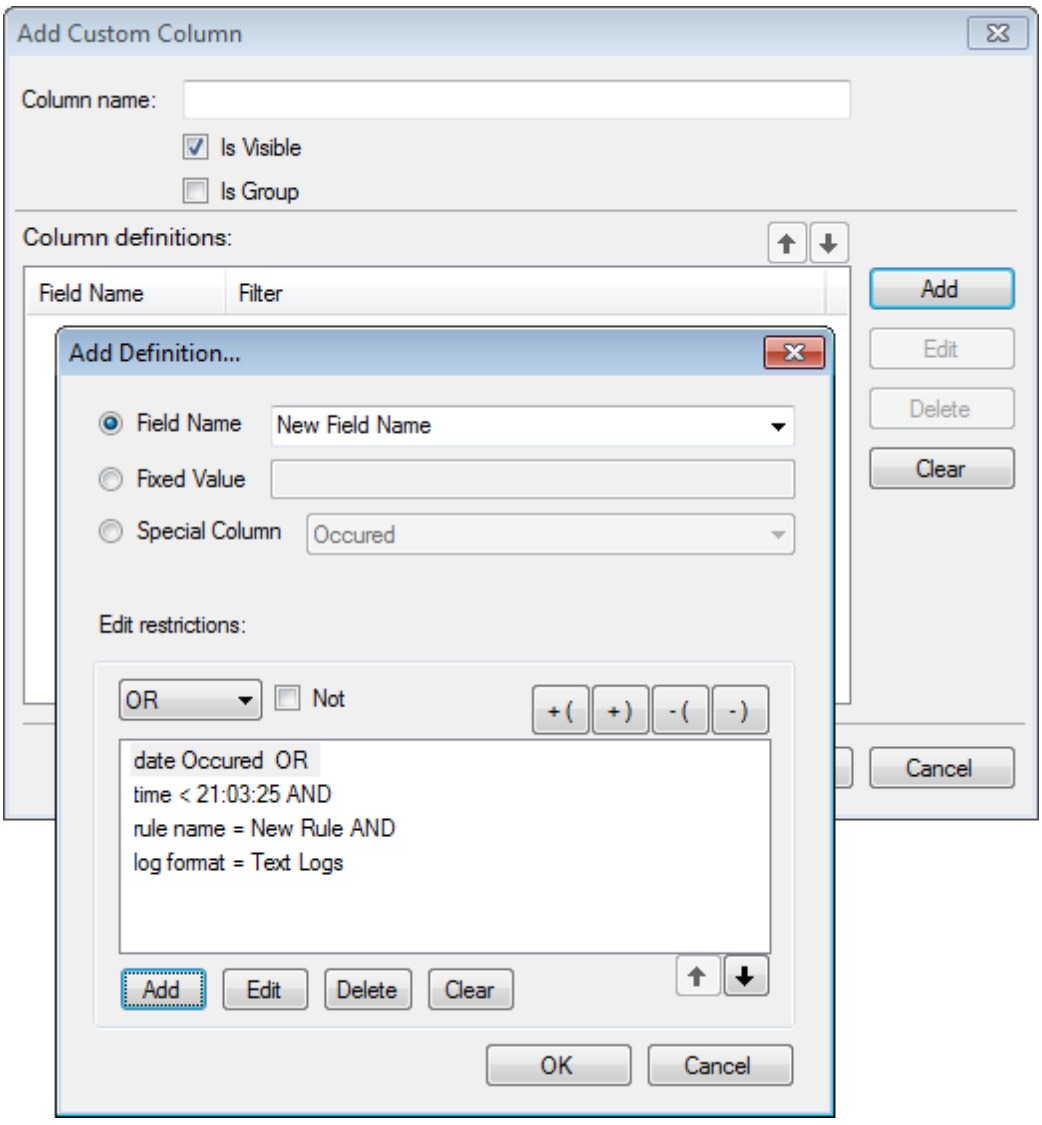
Opción	Description
Print	Utilice la opción **Print** para ver una vista previa de impresión, configurar parámetros de la impresora e imprimir el informe seleccionado.
Open	Utilice el botón **Open** para abrir el informe seleccionado en un navegador. GFI EventsManager utiliza su navegador predeterminado para ver informes en formato HTML.
Open File Location	**Open File Location** le permite acceder a la carpeta que contiene el informe para fines de alma-cenamiento o copias de seguridad.
Export to PDF	Utilice **Export to PDF** para exportar el informe seleccionado en formato de documento portátil.
Suprimir	Haga clic en **Delete** para quitar de la lista un informe generado.

8.8 Definir encabezados de columna

GFI EventsManager le permite crear columnas personalizadas a través del cuadro de diálogo **Add Custom Columns**. Este cuadro de diálogo le permite especificar condiciones, crear un campo nuevo y agregarlos a su informe. También según las condiciones, este cuadro de diálogo le permite personalizar más eficientemente los informes existentes o nuevos.

Para agregar columnas personalizadas:

1. En la ficha **Reporting > Actions**, haga clic en **Create Report**.
2. Haga clic en la ficha **Layout >Add Existing Column** para agregar columnas predeterminadas.
3. Haga clic en **Add Existing Column** para iniciar el cuadro de diálogo **Add Custom Columns**.



Captura de pantalla 130: Definir condiciones de columnas personalizadas

4. En el cuadro de diálogo **Add Custom Column**, haga clic en **Add**.
5. En el cuadro de diálogo **Add Definition...**, configure las opciones que se describen a continuación:

Tabla 61: Opciones para agregar definiciones de columna

Opción	Description
Field Name	Especifique un nombre para el nuevo campo.

Opción	Description
Fixed Value	Seleccione **Fixed Value** si el valor del nuevo campo será fijo. Especifique un valor como un nombre de campo. Por ejemplo, para verificar que siempre se generen los eventos después de las 5 p. m., especifique 5 como valor fijo en lugar de definir un campo de hora y asignar un valor de 5.
Special Column	Las columnas especiales son columnas predefinidas que se pueden utilizar en su condición.
Edit restrictions	Esta sección le permite agregar, editar o eliminar las restricciones de los campos.

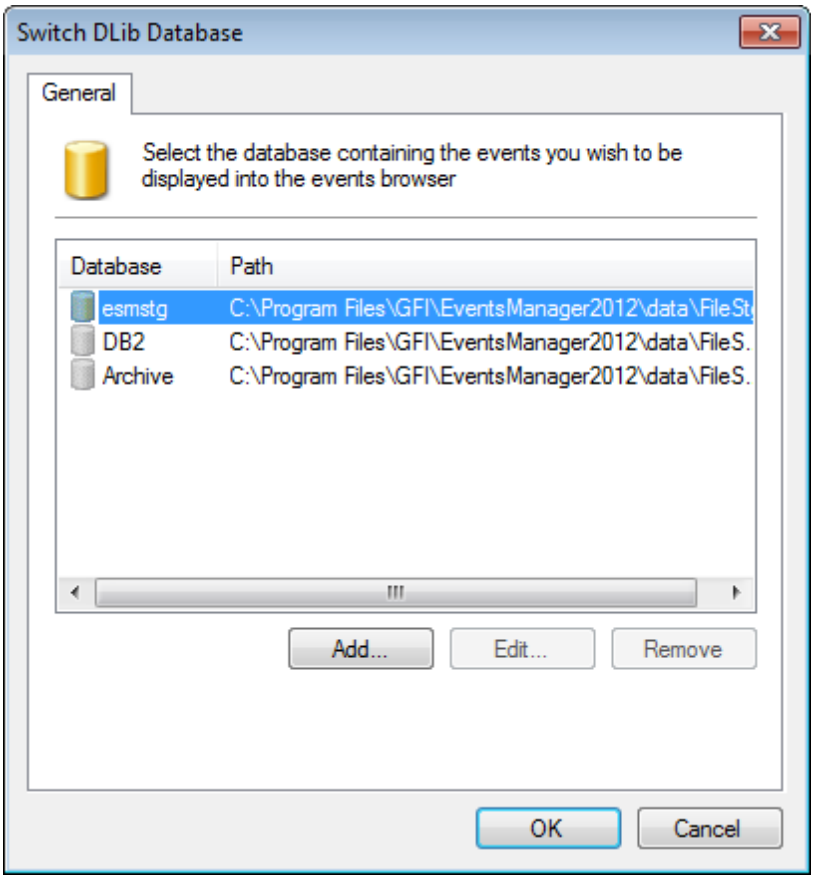
6. Haga clic en **Apply** y **OK**.

8.8.1 Generar informes de eventos de distintas bases de datos

Para los informes, GFI EventsManager le permite cambiar entre diferentes bases de datos. Utilice esta función para informar sobre los eventos que se exportaron/archivaron para su posterior análisis o que se almacenaron en diferentes bases de datos.

Para cambiar de base de datos:

1. En la ficha **Reports> Common Tasks**, haga clic en **Switch database**.



Captura de pantalla 131: Cuadro de diálogo Switch database

2. Seleccione la base de datos de la lista de bases de datos y haga clic en **OK**. Haga clic en **Add…** para especificar un nuevo nombre de base de datos y su ruta relevante. Haga clic en **Edit...** para editar la información especificada.

8.9 Personalizar informes HTML

Las plantillas de informes HTML son personalizables, lo que le permite adaptar GFI EventsManager más eficientemente para satisfacer sus necesidades diarias. Para editar las plantillas disponibles, se requieren conocimientos de HTML y CSS.

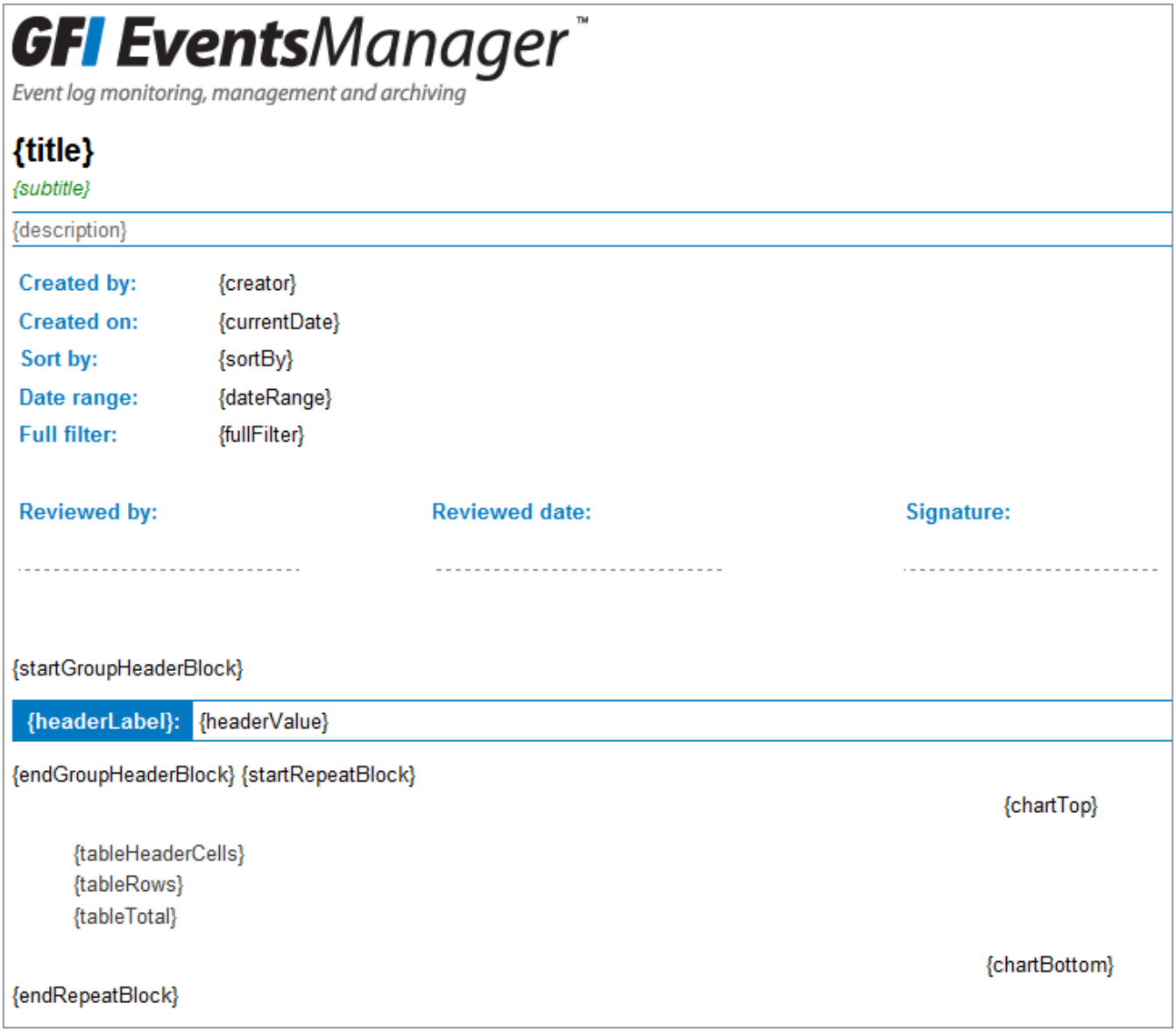
Importante

Antes de editar la plantilla de informe predeterminada, guarde una copia del original para que pueda volver fácilmente a la predeterminada para la resolución de problemas.

Para editar el diseño de informes HTML:

1. Vaya al directorio de instalación de GFI EventsManager:

```
%Program Files\GFI\EventsManager2012\Data\Templates\DefaultReportLayout
```



Captura de pantalla 132: Editar plantillas de informes HTML

2. En la carpeta **DefaultReportLayout**, edite las plantillas que se describen a continuación:

Tabla 62: Plantillas HTML predeterminadas

Plantilla	Description
template_ group_ new.html	Esta plantilla se utiliza al generar informes que contienen datos sobre los orígenes agrupados. La agrupación se puede hacer por usuarios, orígenes, datos de eventos y más.

Plantilla	Description
template_ new.html	Utilice esta plantilla para generar informes estadísticos y gráficos que no organizan los datos en grupos.

3. Con un editor de HTML, edite los siguientes elementos de las plantillas:

Tabla 63: Plantilla HTML: Secciones editables

Sección	Description
Logo de informe	Reemplace el logo de GFI EventsManager por un logo de su elección. Agregue más logos o elimínelos por completo de sus informes.
Etiquetas y texto	Cambie el nombre y la posición de las etiquetas de acuerdo con sus necesidades.
Marcadores	A pesar de que usted puede cambiar de posición los marcadores en el informe, si les cambia el nombre, el motor de informes de GFI EventsManager dejará de generar los datos respectivos.

Los marcadores disponibles incluyen:

Tabla 64: Marcadores de plantilla de informes HTML

Marcador	Description
{title}	Título del informe.
{subtitle}	Subtítulo del informe.
{description}	Descripción del informe.
{creator}	Usuario que generó el informe.
{currentDate}	Fecha en que se genera el informe.
{sortBy}	Ordenar campo.
{dateRange}	Los datos del informe se recopilan a partir del período de tiempo especificado.
{fullFilter}	Lista de restricciones definidas para el informe.
{startGroupHeaderBlock}	Principio de la sección de encabezado del bloque repetitivo.
{headerLabel}	Nombre de encabezado del grupo.
{headerValue}	Valor de encabezado del grupo.
{endGroupHeaderBlock}	Fin de la sección de encabezado del bloque repetitivo.
{startRepeatBlock}	Principio de la sección de cuerpo del bloque repetitivo.
{tableHeaderCells}	La sección de encabezado de los datos de la tabla.
{tableRows}	La sección de cuerpo de los datos de la tabla.
{tableTotal}	Para gráficos. Contiene la suma o el valor de recuento del campo calculado.
{chartTop}	Coloca el gráfico al principio del informe.
{chartBottom}	Coloca el gráfico al final del informe.
{endRepeateBlock}	Fin de la sección de cuerpo del bloque repetitivo.

4. Guarde la plantilla HTML y genere un informe usando el nuevo diseño. Para obtener más información, consulte Generar informes (página 164).

Nota

Si se usan las mismas convenciones HTML/CSS que las plantillas HTML, también puede crear sus propias plantillas personalizadas. Copie la plantilla, cámbiele el nombre y vuelva a utilizar los mismos marcadores.

9 Reglas de procesamiento de eventos

Durante el procesamiento de eventos, GFI EventsManager ejecuta un conjunto de reglas configurable en los registros recopilados, con el fin de clasificar los eventos y activar las alertas/acciones según corresponda. De forma predeterminada, GFI EventsManager viene con un conjunto preconfigurado de reglas de procesamiento de eventos que le permite obtener control de toda la red sobre los registros del equipo, con un esfuerzo de configuración mínimo. También puede modificar estas reglas predeterminadas o crear otras adaptadas a las necesidades de su organización.

Temas de este capítulo:

9.1 Acerca de las reglas de procesamiento de eventos 179

9.2 Administrar carpetas de conjuntos de reglas 181

9.3 Crear nuevas reglas de procesamiento de eventos 184

9.4 Crear nuevas reglas desde eventos existentes 189

9.5 Parámetros de filtro avanzado de eventos 194

9.6 Priorizar reglas de procesamiento de eventos 195

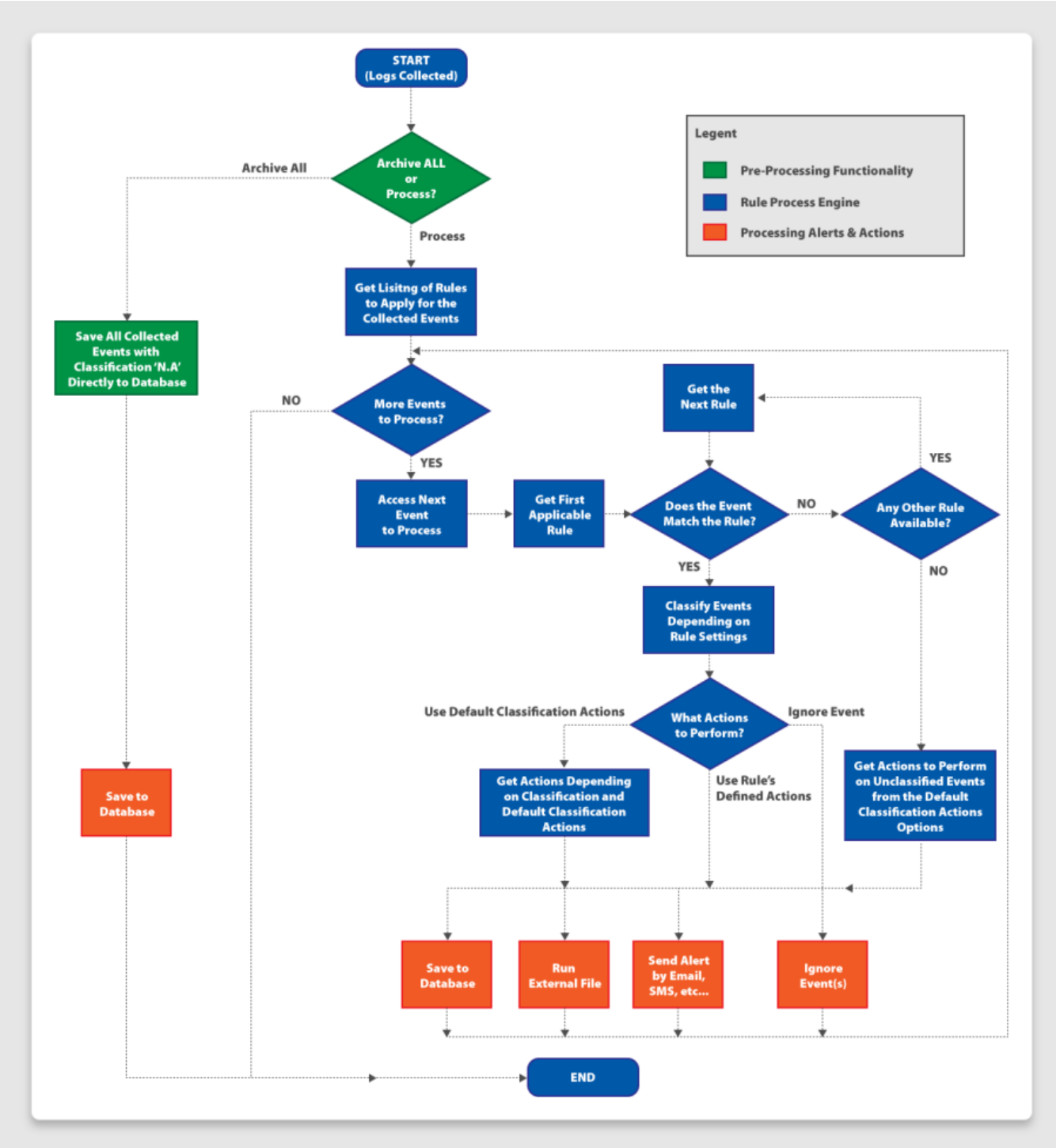
9.1 Acerca de las reglas de procesamiento de eventos

Las reglas de procesamiento de eventos son comprobaciones que se ejecutan contra los registros de eventos cuando estos se recopilan. Según las condiciones configuradas en una regla, las reglas de procesamiento de eventos lo ayudan a:

- **Clasificar eventos procesados**: se asigna una clasificación de gravedad a los registros recopilados. Esto le permite activar acciones o notificaciones si se procesa un determinado registro de gravedad. De forma predeterminada, los eventos se clasifican según cinco clasificaciones principales; sin embargo, es posible agregar más clasificaciones.
- **No incluir el ruido (sucesos repetidos) o eventos no deseados**: se eliminan los registros duplicados o los registros que no son importantes para usted y se archivan solamente los datos de los eventos importantes. Esto reduce el crecimiento de la base de datos y reduce el espacio de almacenamiento.
- **Activar alertas por correo electrónico, SMS o la red cuando se producen eventos clave**: se envían notificaciones a los destinatarios configurados cuando se detectan determinados eventos. Puede configurar una regla de procesamiento de eventos para enviar notificaciones a los destinatarios cuando se cumplan las condiciones de la regla.
- **Intentar acciones correctivas**: se ejecutan los archivos ejecutables, los comandos y las secuencias de comando cuando se detectan eventos específicos. Esto le permite implementar automáticamente acciones correctivas para mitigar o eliminar por completo un problema detectado.
- **Filtrar eventos que coinciden con criterios específicos**: se eliminan los registros de eventos que no son importantes para usted. Por ejemplo, puede ejecutar una regla que no incluya los eventos duplicados o de baja gravedad.
- **Archivar eventos filtrados**: el archivado de eventos se basa en la gravedad del evento y en las opciones de configuración de las reglas de procesamiento de eventos. Por ejemplo: puede

configurar GFI EventsManager para que archive solamente los eventos que están clasificados como críticos o de alta gravedad y descartar todos los demás.

El siguiente diagrama de flujo ilustra las etapas de procesamiento de eventos que lleva a cabo GFI EventsManager:



Captura de pantalla 133: Cómo funcionan las reglas de procesamiento de eventos

9.1.1 Clasificación de eventos

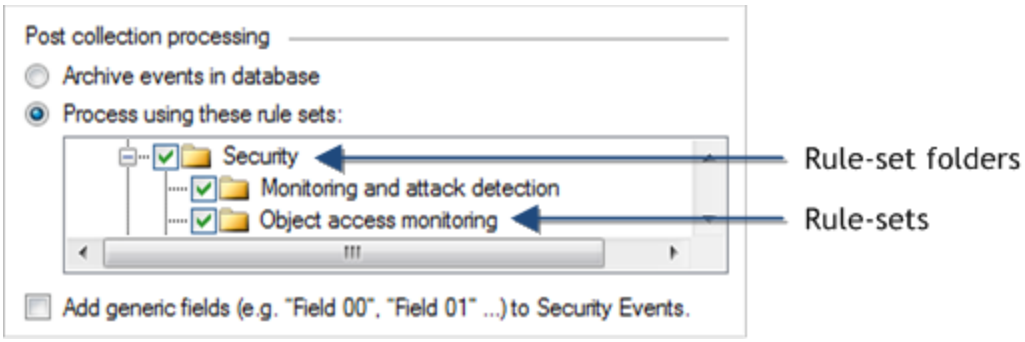
La clasificación de eventos se basa en la configuración de las reglas que se ejecutan en los registros recopilados. Los eventos que no cumplen con una condición de clasificación de eventos se etiquetan

como sin clasificar. Los eventos sin clasificar también se pueden usar para activar las mismas alertas y acciones disponibles para los eventos clasificados.

GFI EventsManager clasifica los eventos en los niveles de importancia estándar, como crítica, alta, media, baja y ruido (entradas de registro no deseadas o repetidas).

9.2 Administrar carpetas de conjuntos de reglas

En GFI EventsManager las reglas de procesamiento de eventos se organizan en conjuntos de reglas, y cada conjunto de reglas puede contener una o más reglas especializadas que se pueden ejecutar en los registros recopilados.



Captura de pantalla 134: Carpeta de conjuntos de reglas y conjuntos de reglas

Los conjuntos de reglas se organizan también en carpetas de conjuntos de reglas. De esta manera, puede agrupar los conjuntos de reglas de acuerdo con las funciones y acciones que realizan las reglas respectivas. De forma predeterminada, GFI EventsManager viene con carpetas preconfiguradas, conjuntos de reglas y reglas de procesamiento de eventos que se pueden personalizar incluso más para adaptarlas a sus necesidades de procesamiento de eventos.

Este tema contiene información sobre:

- Conjuntos de reglas disponibles
- Agregar una carpeta de conjuntos de reglas
- Renombrar y eliminar carpetas de conjuntos de reglas

9.2.1 Conjuntos de reglas disponibles

La siguiente tabla proporciona las carpetas de conjuntos de reglas disponibles al instalar GFI EventsManager. Cada carpeta de conjunto de reglas contiene varias reglas y/o conjuntos de reglas de procesamiento de eventos:

Tabla 65: Carpetas de conjuntos de reglas comunes disponibles

Carpeta de conjunto de reglas	Descripción
Eventos de Windows	Contiene reglas adaptadas para servidores y estaciones de trabajo de Windows®, entre las que se incluyen: » Reglas de reducción de ruido » Reglas de requisitos de PCI DSS » Reglas de seguridad » Reglas de estado del sistema » Reglas de aplicación de seguridad » Reglas del servidor de infraestructura » Reglas del servidor de bases de datos » Reglas de servidor web » Reglas del servidor de impresión » Reglas de GFI » Reglas de servicios de terminal » Reglas del servidor de correo electrónico » Reglas de replicación de archivos » Reglas del servicio de directorio » Reglas personalizadas » Reglas de informes » Reglas de auditoría de SharePoint
Registros de texto	Contiene reglas adaptadas al procesamiento de los protocolos de transferencia web. Estos incluyen: » Reglas HTTP » Reglas FTP » Reglas SMTP
Mensajes syslog	Contiene reglas adaptadas al procesamiento de los registros de sistema de LINUX y UNIX. Estos incluyen: » Reglas de hosts de Linux\Unix » Reglas de redes Juniper » Reglas de Cisco PIX y ISA » Reglas según la gravedad » Reglas de IBM iSeries
Capturas SNMP	Contiene reglas adaptadas a la mensajería de capturas SNMP. Estas incluyen: » Reglas de Cisco IOS versión 12.1 (11) MIB » Reglas de Cisco IOS versión 12.1 (14) MIB » Reglas de Cisco IOS versión 12.2 (20) MIB » Reglas de Cisco IOS versión 12.2 (25) MIB » Reglas de Allied Telesis AT-AR-700 Family

Carpeta de conjunto de reglas	Descripción
Auditorías SQL Server®	Contiene reglas adaptadas a la supervisión de auditorías de SQL Server®. Estas incluyen: » Reglas de reducción de ruido » Reglas de cambios de base de datos » Reglas de cambios de servidor » Reglas de inicio/cierre de sesión » Reglas de SQL Server® » Reglas de acceso a las bases de datos
Auditorías de Oracle	Contiene reglas adaptadas para la supervisión de auditorías de Oracle Server. Estas incluyen, entre otras: » Reglas de reducción de ruido » Reglas de cambios de base de datos » Reglas de cambios de servidor » Reglas de inicio/cierre de sesión » Reglas de cambios en la seguridad
Comprobaciones de supervisión	Contiene reglas que le permiten supervisar los mensajes de supervisión activa. Se incluyen reglas relacionadas con el conjunto predeterminado de reglas de supervisión. Las comprobaciones de supervisión generan registros de eventos. Las reglas de procesamiento de eventos pueden procesar estos registros de eventos para activar una acción o una notificación cuando se detecta un error.

9.2.2 Agregar una carpeta de conjuntos de reglas

Para crear una nueva carpeta de conjunto de reglas:

1. Haga clic en la ficha **Configuration** y seleccione **Event Processing Rules**.
2. En **Common Tasks**, seleccione **Create folder**.
3. Especifique un nombre único para la nueva carpeta de conjuntos de reglas.

> **Nota**
>
> Para crear carpetas de conjunto de reglas secundarias, haga clic con el botón secundario en la carpeta principal y seleccione **Create new folder…**.

9.2.3 Renombrar y eliminar una carpeta de conjunto de reglas

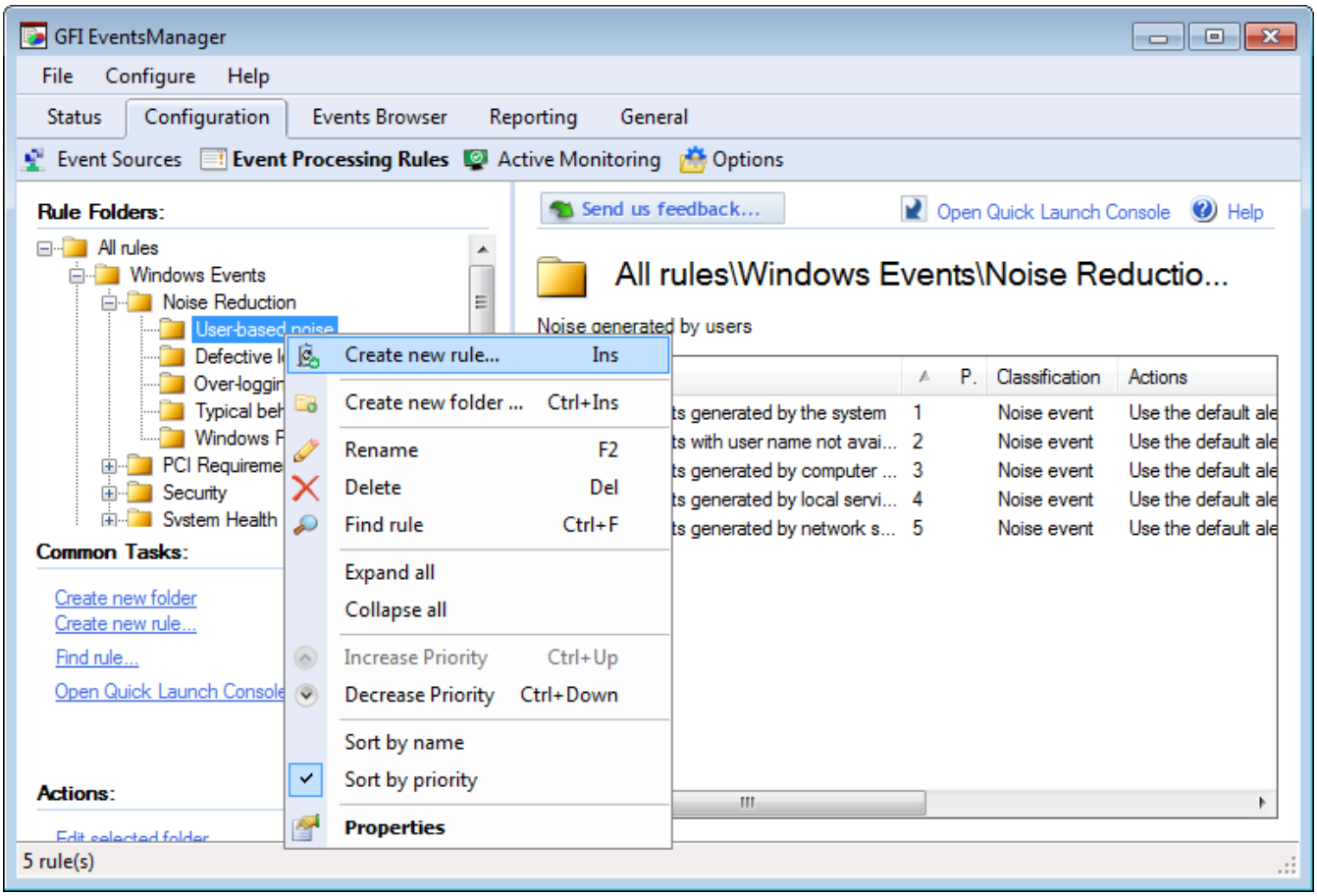
Para cambiar el nombre o eliminar carpetas de conjunto de reglas existentes, haga clic con el botón secundario en la carpeta de conjunto de reglas de destino y seleccione **Rename** o **Delete**, según corresponda.

> **Importante**
>
> Eliminar una carpeta de conjunto de reglas genera la eliminación de todas las reglas y conjuntos de reglas incluidos en la carpeta eliminada.

9.3 Crear nuevas reglas de procesamiento de eventos

Para crear una nueva regla de procesamiento de eventos:

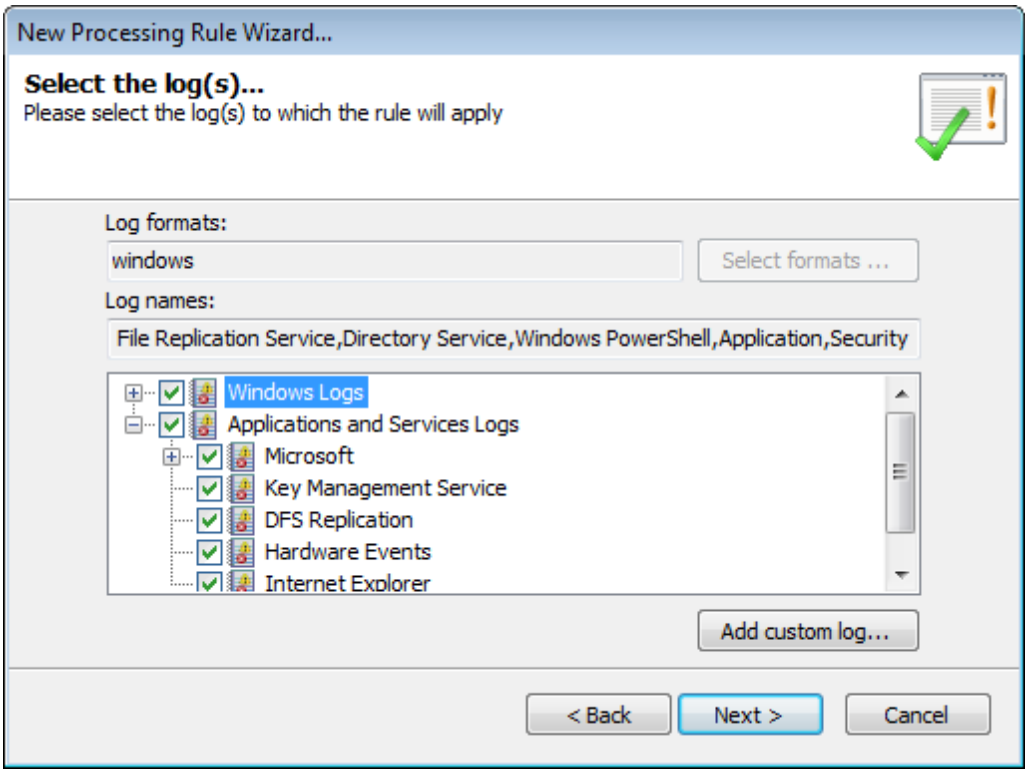
1. Haga clic en la ficha **Configuration > Event Processing Rules**.



Captura de pantalla 135: Crear una nueva regla

2. Haga clic con el botón secundario en el conjunto de reglas donde se creará la nueva regla y haga clic en **Create new rule...**.

3. Especifique el nombre y la descripción (opcional) de la nueva regla. Haga clic en **Siguiente**.



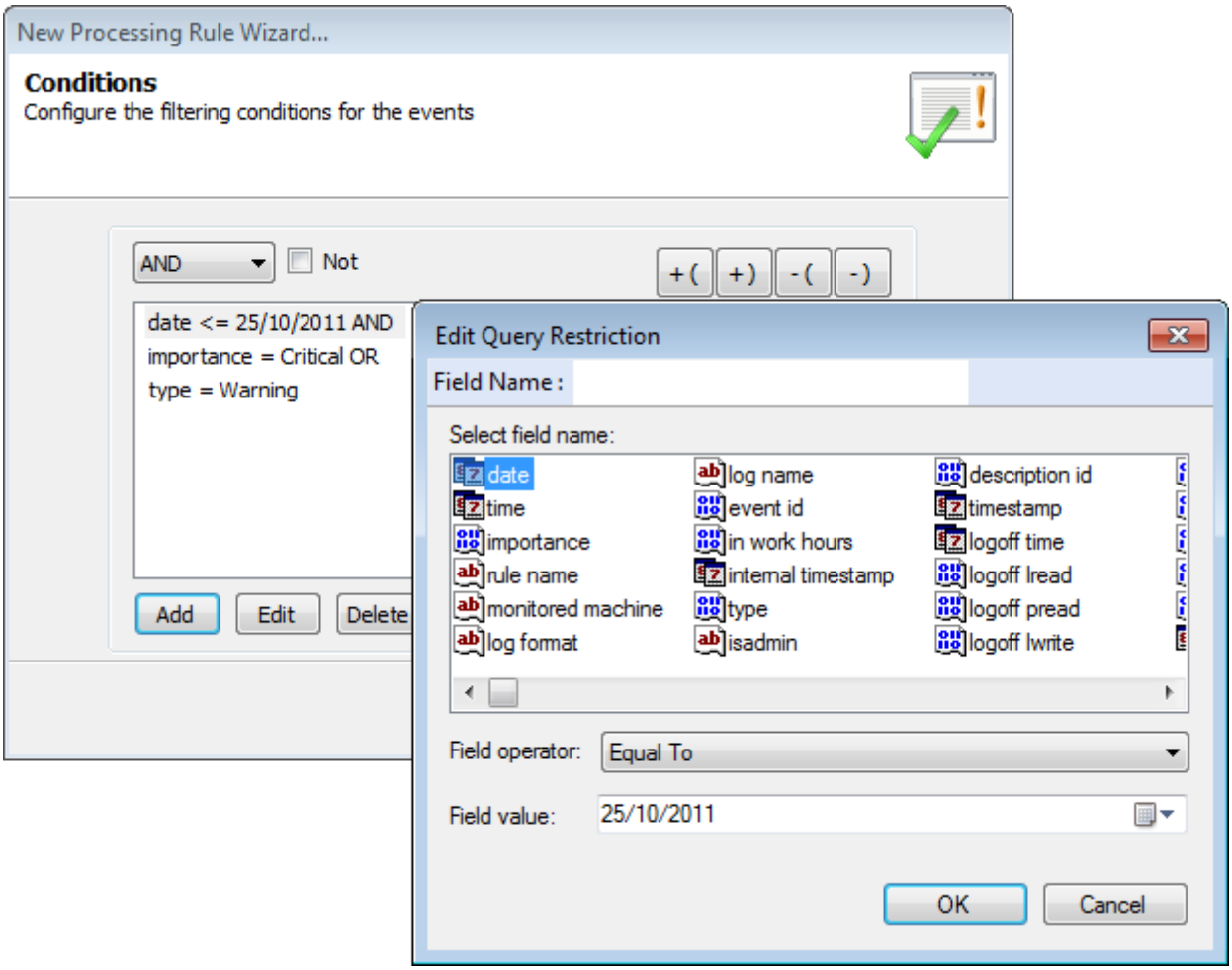
Captura de pantalla 136: Seleccionar los registros a los que se aplicará la regla

4. Seleccione los registros de eventos a los que aplica la regla.

5. (Opcional) Haga clic en **Add custom log…** para insertar un registro de eventos preconfigurado. Haga clic en **Next**. Para obtener más información, consulte Recopilar eventos personalizados.

Nota

Para las auditorías SQL, las auditorías Oracle, los registros de texto y las capturas SNMP, especifique la ruta de acceso completa a la carpeta de registro del objeto. Por ejemplo: “**C:\W3C\logs**”.



Captura de pantalla 137: Configurar condiciones de la regla

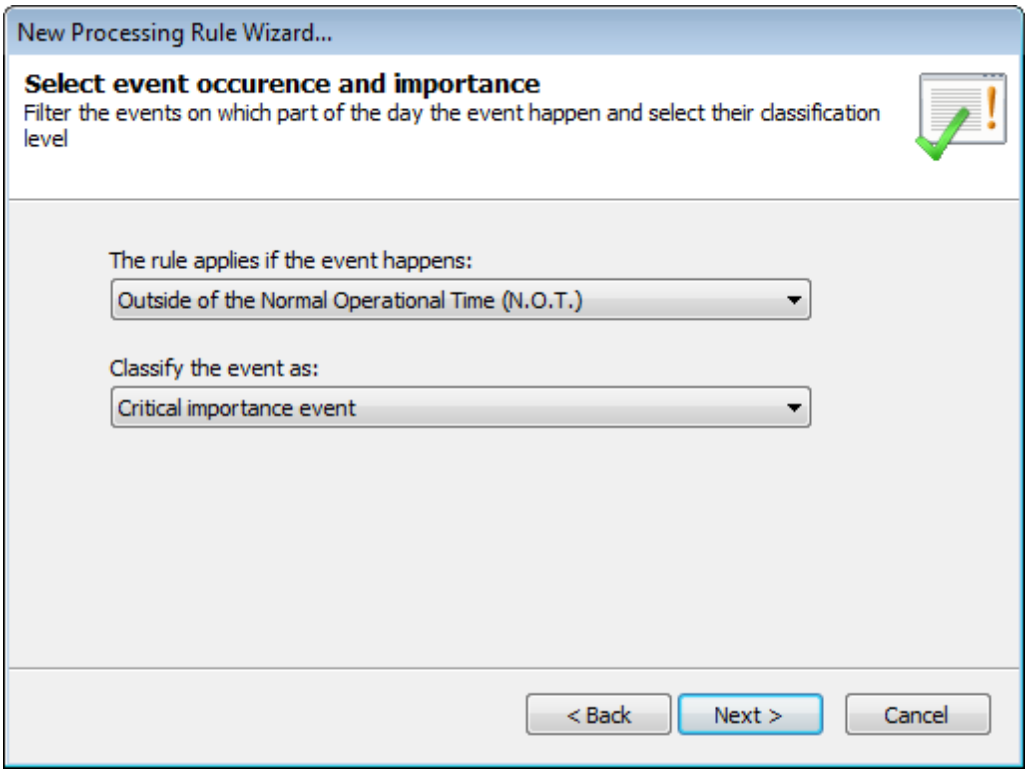
6. Haga clic en **Add** para seleccionar un campo en el que desea basar la condición de consulta. Para el campo seleccionado, especifique **Field Operator** y **Field Value**. Haga clic en **OK** para aceptar.

Nota

Repita este paso hasta seleccionar todos los campos obligatorios. Para obtener más información, consulte Diseñar restricciones de consulta.

Nota

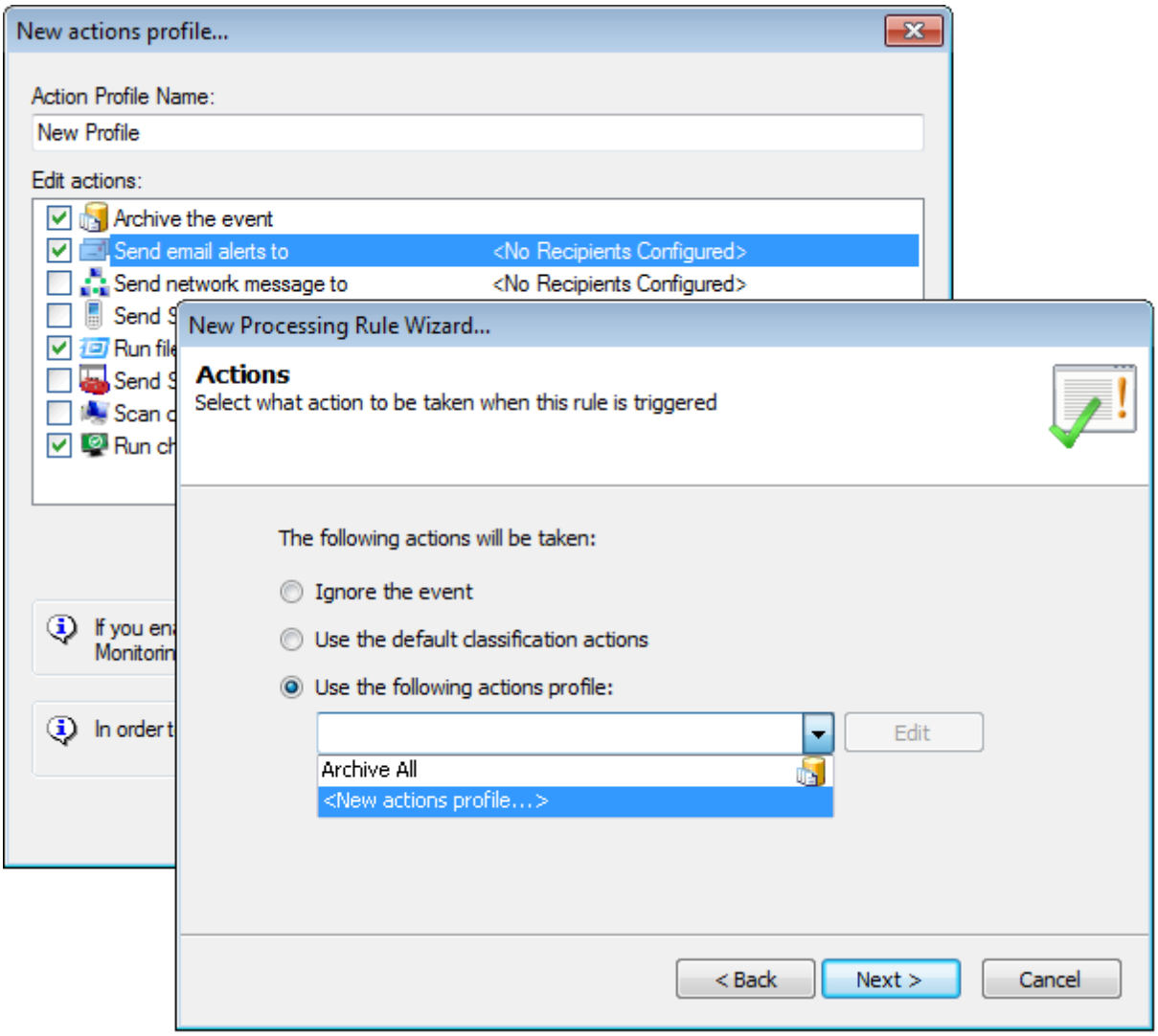
Para filtrar los eventos que hacen referencia a un usuario administrador (eventos con el identificador de seguridad SID, que identifica una sesión de inicio de administrador), asegúrese de que, si el origen del evento es un miembro de dominio, también se agregue el controlador de dominio como un origen de eventos. Para obtener más información, consulte Crear un nuevo grupo de orígenes de eventos.


New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
Outside of the Normal Operational Time (N.O.T.)
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Captura de pantalla 138: Seleccionar ocurrencia e importancia del evento

7. Especifique el tiempo en que la regla es aplicable. Ejemplo: en cualquier momento, durante las horas laborales o no laborales. Las horas laborales y no laborables se basan en los parámetros de tiempo de funcionamiento configurados para sus orígenes de eventos. Para obtener más información, consulte Configurar tiempo operativo de los orígenes de eventos.

8. Seleccione la clasificación (crítica, alta, media, baja o ruido) que se asignará a los eventos que cumplan con las condiciones establecidas en esta regla. Haga clic en **Siguiente**.



Captura de pantalla 139: Seleccionar acción activada

9. Especifique qué acciones activa esta regla y haga clic en **Next**. Las acciones disponibles son:

Tabla 66: Configurar nuevas reglas de procesamiento de eventos: Acciones

Acción	Descripción
Ignore the event	Seleccione esta opción para que GFI EventsManager ignore el evento y no genere una acción o notificación.
Use the default classification actions	Seleccione esta opción para usar las opciones preconfiguradas en **Default Classification Actions**.

Acción	Descripción
Use the following actions profile	El perfil Archive All se agrega de forma predeterminada. Para crear un nuevo perfil: 1. En el menú desplegable, seleccione **<Nuevo perfil de acción>**. Esto inicia el cuadro de diálogo **New actions profile...**. 2. Especifique un nombre para el nuevo perfil en el cuadro de texto **Action Profile Name**. 3. Seleccione las acciones que desea que realice el perfil. Las siguientes acciones se encuentran disponibles: » Archive the event » Send email alerts to » Send network message to » Send SMS message to » Run file » Send SNMP Message » Scan computer » Run checks on computer **Nota** Si se selecciona Run checks on computer, asegúrese de que las comprobaciones de supervisión estén habilitadas en el equipo. Para obtener más información, consulte Configurar supervisión de orígenes de eventos. 4. Para cada acción que seleccione, haga clic en **Configure** para configurar los parámetros.

10. Haga clic en **Apply** y **OK**.

Nota

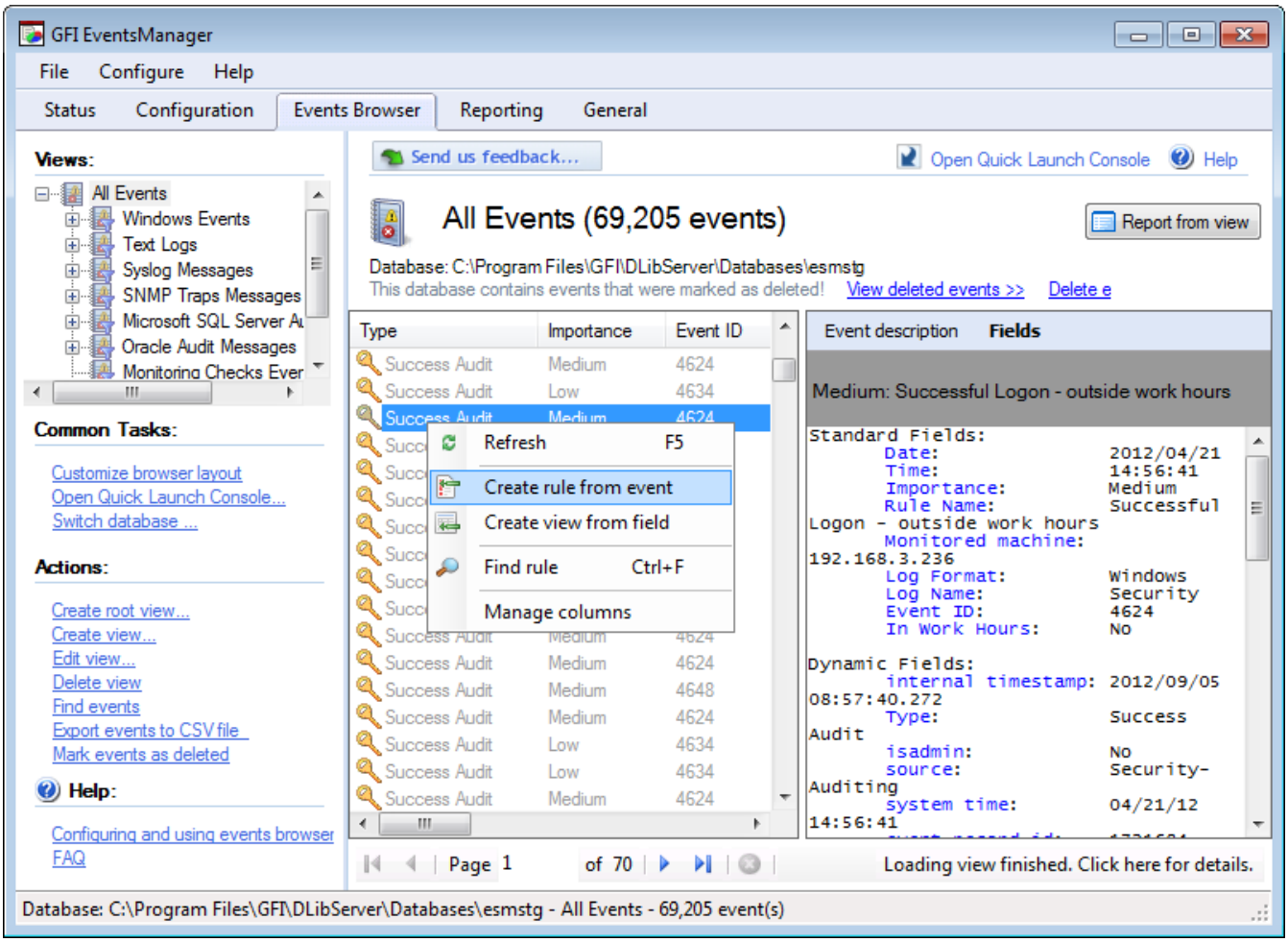
Asigne las nuevas reglas a sus orígenes de eventos. Para obtener información sobre cómo recopilar registros de eventos y procesarlos mediante las reglas de procesamiento de eventos especificadas, consulte Recopilar registros de eventos.

9.4 Crear nuevas reglas desde eventos existentes

GFI EventsManager le permite crear nuevas reglas en base a la información de eventos existentes.

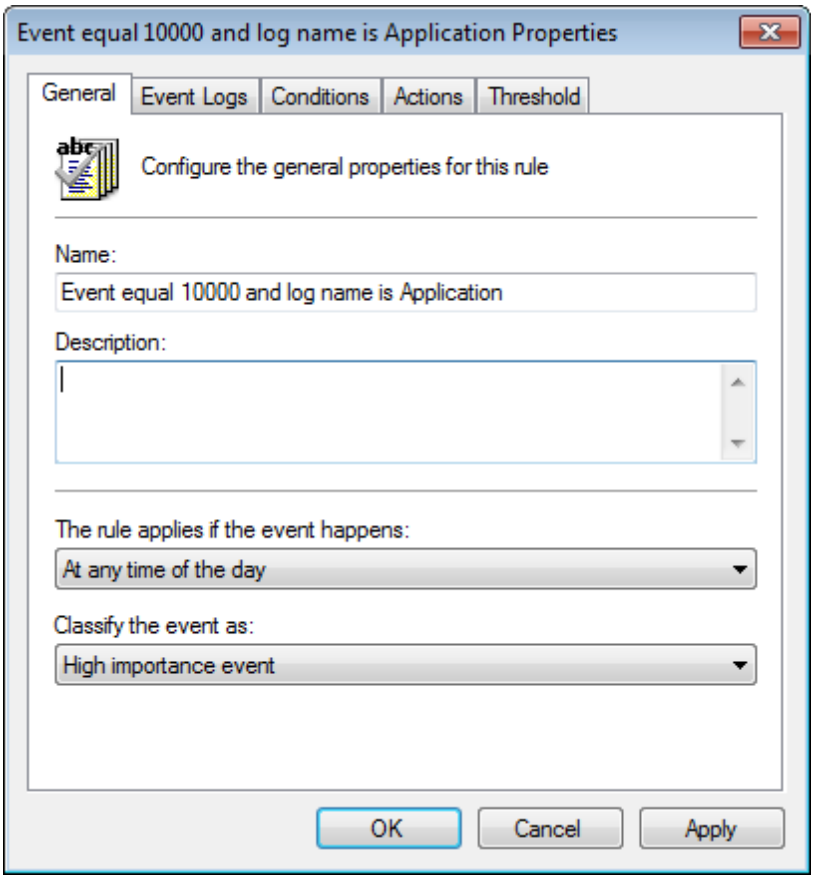
Para crear una nueva regla a partir de un evento existente:

1. En el **Explorador de eventos**, busque el registro de eventos en el que desea basar la regla.



Captura de pantalla 140: Crear una regla a partir de un evento existente

2. Haga clic con el botón secundario en el evento y seleccione **Create rule from event**.



Captura de pantalla 141: Nueva regla a partir de un evento - Configuración general

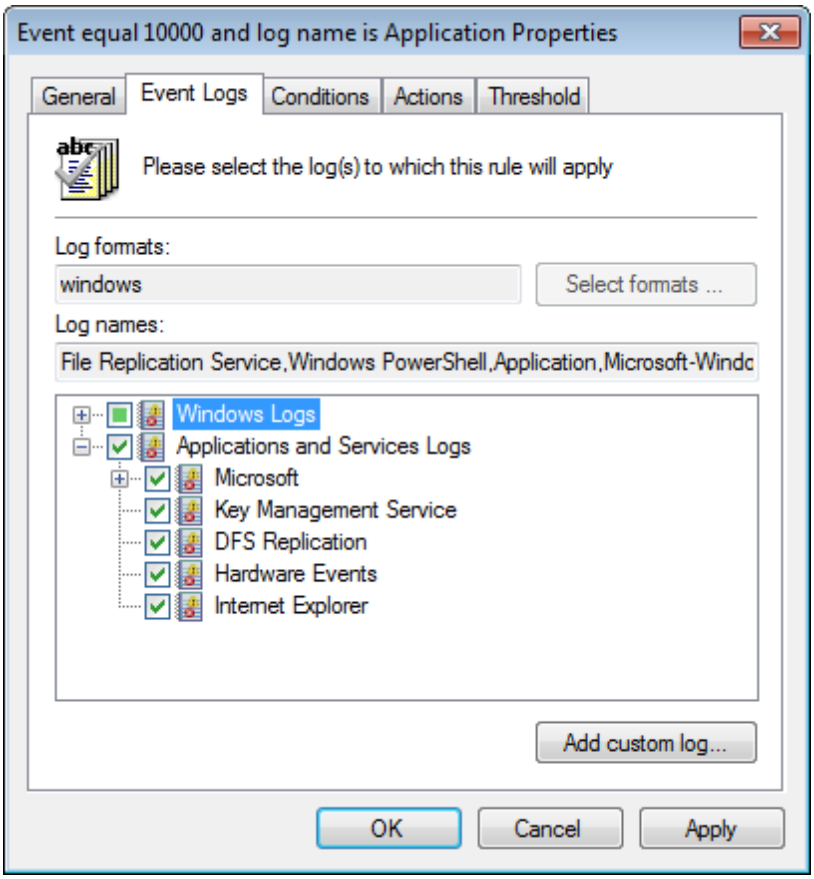
3. Especifique un nombre único y una descripción opcional para la nueva regla.

4. En el menú desplegable **The rule applies if the event happens**, seleccione el momento en que la regla es aplicable. Seleccione una de las siguientes opciones:

- At any time of the day (para cualquier momento del día)
- During Normal Operational Time (para el tiempo operativo normal)
- Outside the Normal Operational Time (fuera del tiempo operativo normal)

> **Nota**
>
> Para obtener más información, consulte Configurar tiempo operativo de los orígenes de eventos.

5. En el menú desplegable **Classify the event as**, seleccione el nivel de clasificación que desea asignar al evento cuando se genere.

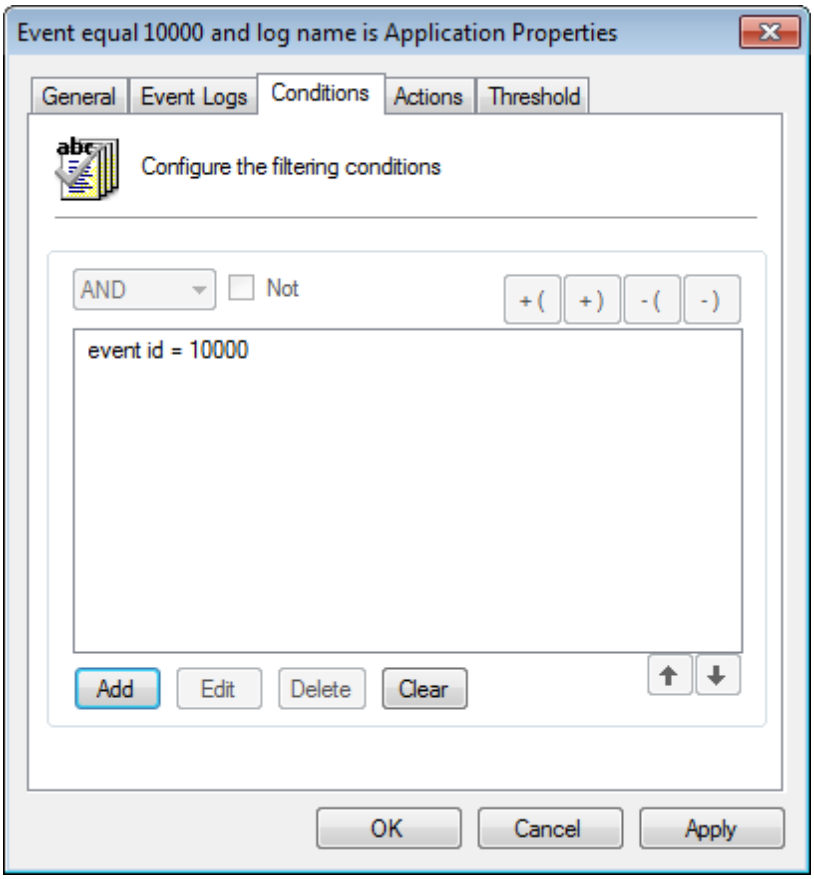


Captura de pantalla 142: Nueva regla a partir de un evento - Seleccionar registros que desea recopilar

6. En la ficha **Event Logs**, seleccione los registros que desea recopilar. Para agregar registros personalizados, haga clic en **Add custom log...**, especifique el nombre del registro personalizado y haga clic en **OK**.

Nota

Para obtener más información, consulte Recopilar registros personalizados.



Captura de pantalla 143: Nueva regla a partir de un evento - Agregar condiciones

7. Haga clic en la ficha **Conditions**.Haga clic en **Add** para seleccionar un campo en el que desea basar la condición de consulta. Para el campo seleccionado, especifique **Field Operator** y **Field Value**. Haga clic en **OK** para aceptar.

> **Nota**
>
> Repita este paso hasta seleccionar todos los campos obligatorios. Para obtener más información, consulte Diseñar restricciones de consulta.

8. Haga clic en la ficha **Actions** y seleccione la acción que se debe realizar cuando se active la regla. Las opciones disponibles se describen a continuación:

Tabla 67: Acciones disponibles de reglas de procesamiento de eventos

Opción	Descripción
Ignore the event	Ignora el evento hasta que se genera una nueva instancia del evento.
Use the default classification actions	Se usan las acciones configuradas en Default Classification Actions. Para obtener más información, consulte Configurar acciones de clasificación predeterminadas.
Use the following actions profile	En el menú desplegable, seleccione un perfil o <Nuevo perfil de acción> y haga clic en **Edit** para configurar el perfil de la acción.

9. Haga clic en la ficha **Threshold** y configure el valor del umbral de evento. Es decir, el número de veces que se debe detectar un evento antes de activar las alertas y acciones correctivas. Esto ayuda a reducir los falsos positivos que provoca el ruido (los eventos repetidos) en sus registros de eventos.

10. Haga clic en **Apply** y **OK**.

9.5 Parámetros de filtro avanzado de eventos

GFI EventsManager le permite a los administradores de sistemas configurar parámetros avanzados de filtrado de eventos. Estas opciones solamente están disponibles para syslogs y registros de eventos de Windows®. Consulte las siguientes secciones para obtener información acerca de:

» Parámetros de filtrado de eventos de Windows®

» Parámetros de filtrado de syslog

9.5.1 Parámetros de filtrado de eventos de Windows®

El campo **Event IDs:** les permite a los administradores de sistemas configurar los parámetros que se describen en la tabla a continuación:

Tabla 68: Parámetros de filtrado de eventos de Windows®: Campo Event ID

Parámetro	Descripción
Single events	Event IDs: 575
List of events	Event IDs: 550, 570
Range of events	Event IDs: 575-600
Combination of events	Event IDs: 550, 570, 575-600

Los campos **Source**, **Category** y **User fields** les permiten a los administradores de sistemas configurar los parámetros que se describen en la tabla a continuación:

Tabla 69: Parámetros de filtrado de eventos de Windows®: Campos Source, Category y User

Parámetro	Descripción
Single source name	Message: session opened
List of sources	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

9.5.2 Parámetros de filtrado de syslog

Los campos **Message** y **Process** les permiten a los administradores de sistemas configurar los parámetros que se describen en la tabla a continuación:

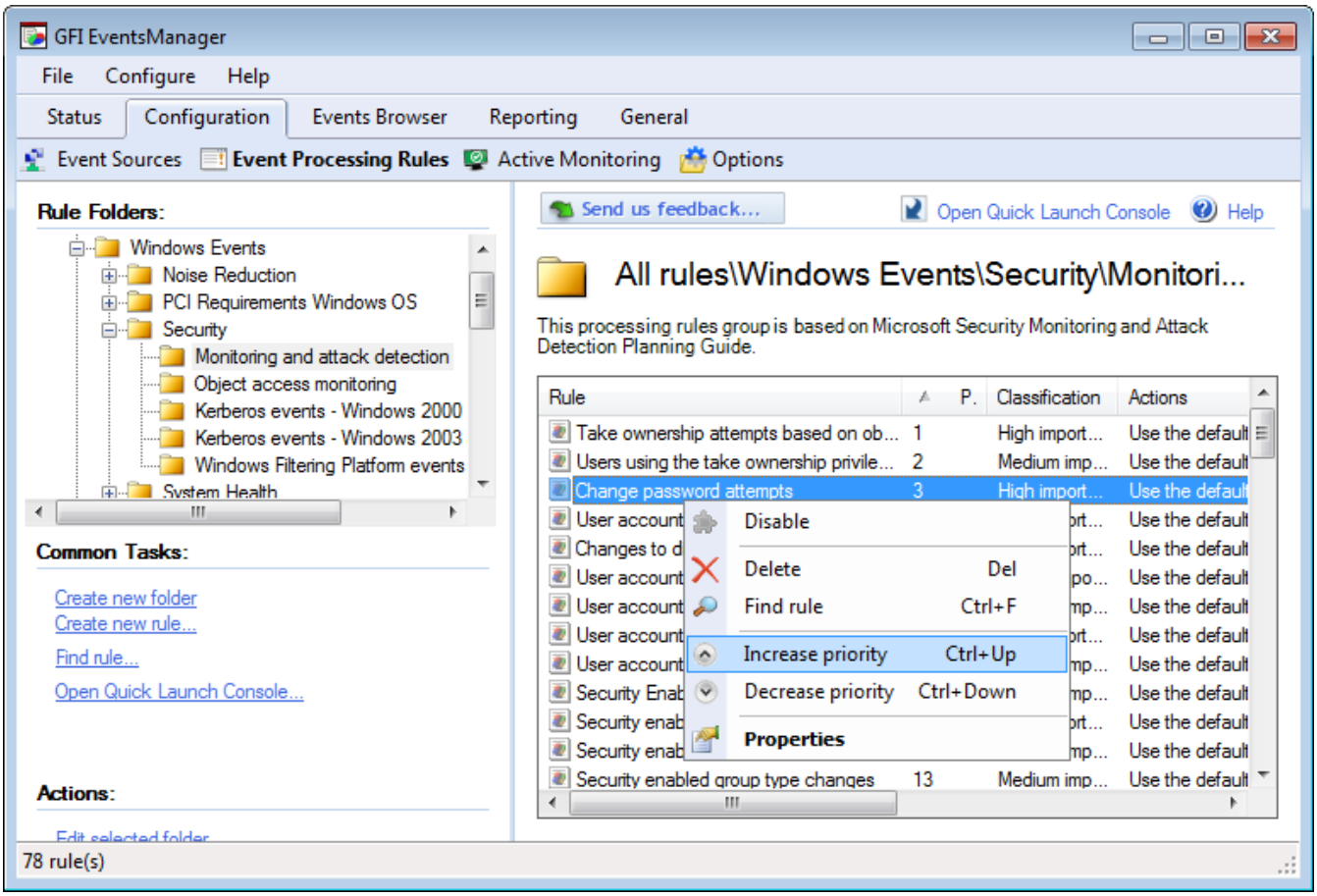
Tabla 70: Parámetros de filtrado de syslog: Campos Message y Process

Parámetros	Descripción
Single message	Message: session opened
List of messages	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

9.6 Priorizar reglas de procesamiento de eventos

Las reglas de procesamiento de eventos se ejecutan en orden de prioridad. Para cambiar el orden de ejecución:

1. En la ficha **Configuration > Events Processing Rules > Rule Folders**, expanda la carpeta de conjunto de reglas.



2. En el panel derecho, haga clic con el botón secundario en una regla y seleccione **Increase priority** o **Decrease priority** para aumentar o reducir la prioridad, según corresponda. O bien, seleccione una regla y presione **Ctrl+Up** para aumentar o **Ctrl+Down** para disminuir la prioridad.

10 Supervisión activa

Los registros de eventos son útiles para hacer un seguimiento de diferentes aspectos operativos de dispositivos, equipos y servidores, pero, en muchos casos, los usuarios necesitan más que simplemente registros para inspeccionar esta actividad con mayor detalle. Para mitigar este problema, GFI EventsManager usa las comprobaciones de supervisión activa. Las comprobaciones de supervisión lo ayudan a detectar errores o irregularidades de forma automática; por lo tanto, es posible identificar y resolver de forma proactiva problemas imprevistos antes de que sucedan.

GFI EventsManager viene con un conjunto de comprobaciones predefinidas, específicamente diseñadas para cumplir con los requisitos de los sistemas operativosWindows®, los sistemas operativos Linux/Unix, los dispositivos SNMP y los protocolos y servicios de red/Internet.

En este capítulo, se brinda información acerca de la administración, la creación y el uso de las comprobaciones de supervisión activa.

Temas de este capítulo:

10.1 Acerca de las comprobaciones de supervisión activa 196

10.2 Crear y configurar una carpeta raíz 198

10.3 Agregar subcarpetas a una carpeta raíz 202

10.4 Crear y configurar comprobaciones de supervisión activa 207

10.5 Aplicar comprobaciones de supervisión activa 213

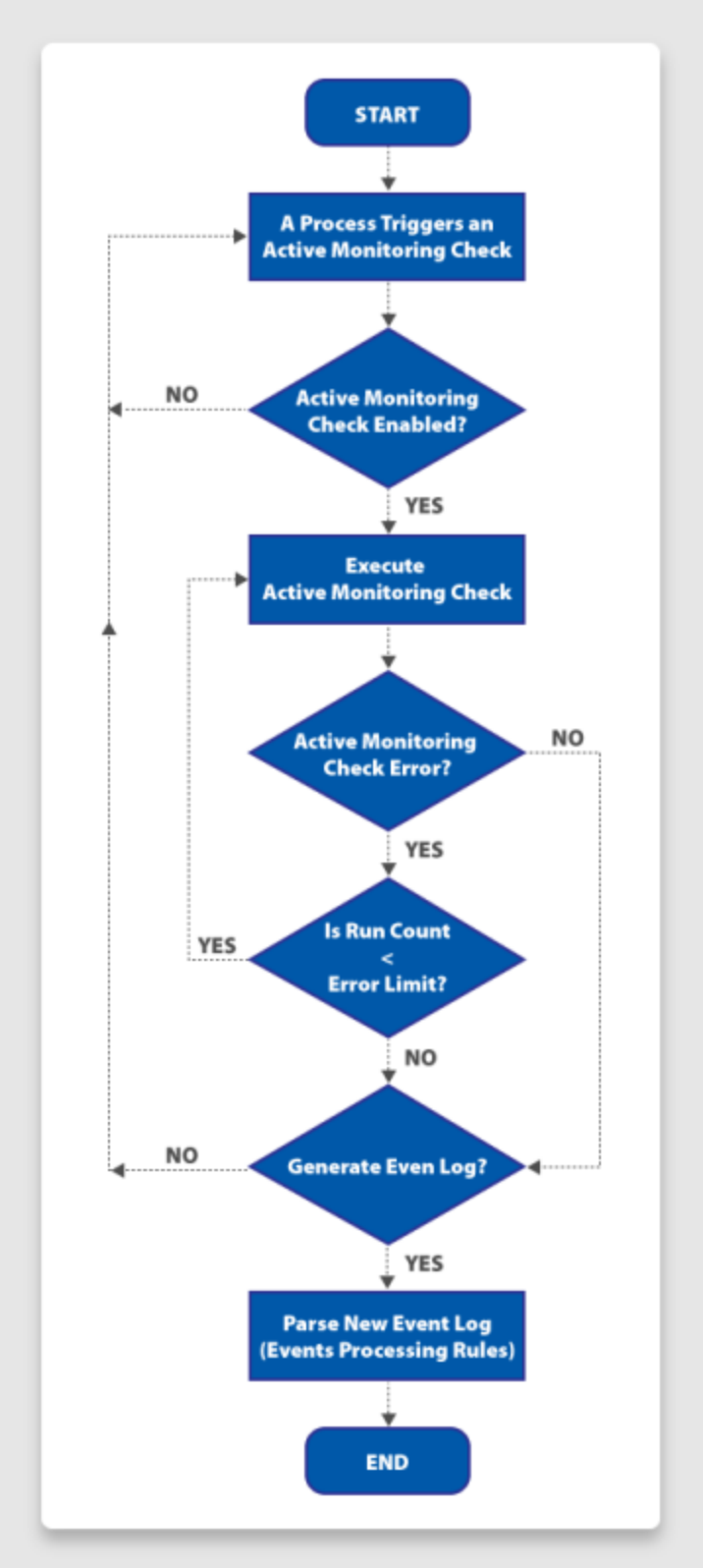
10.6 Eliminar carpetas y comprobaciones de supervisión 215

10.1 Acerca de las comprobaciones de supervisión activa

Una comprobación de supervisión es una regla preconfigurada, que depende de la operación de los componentes o la actividad de un sistema, como el uso de la CPU o las solicitudes de ping, que se usan para comprobar la disponibilidad del sistema. Las comprobaciones de supervisión activa analizan de forma activa los orígenes de eventos para determinar si se cumplen las condiciones de los parámetros configurados.

Independientemente de si una prueba de supervisión falla o tiene éxito, se genera un registro de eventos del equipo que analizó. GFI EventsManager asigna una clasificación de gravedad al registro de evento generado.

Se puede crear una regla de procesamiento de eventos a partir del registro de eventos generado. Las reglas de procesamiento de eventos pueden activar automáticamente alertas, ejecutar comprobaciones adicionales y ejecutar secuencias de comandos y aplicaciones para solucionar el problema que generó el registro.



Captura de pantalla 144: Cómo funcionan las comprobaciones de supervisión activa

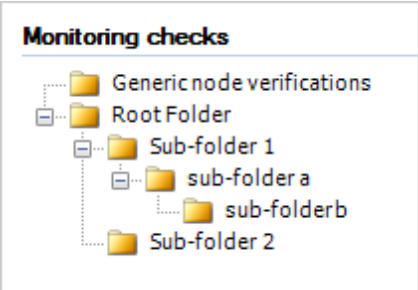
Ejemplo

Configure una comprobación de supervisión para generar un registro de eventos cuando el espacio de disco duro de un equipo alcanza un límite preconfigurado. Para lograr esto:

1. Cuando se alcanza el límite y la comprobación de supervisión genera un evento, búsquela en el Explorador de eventos y cree una regla de procesamiento de eventos basado en este. Para obtener más información, consulte Crear nuevas reglas desde eventos existentes.

2. Configure las nuevas condiciones de reglas del procesamiento de eventos para ignorar eventos que no coincidan. Para obtener más información, consulte Crear nuevas reglas de procesamiento de eventos.

3. Configure la nueva regla para activar una alerta o una acción a fin de resolver el problema. Para obtener más información, consulte Configurar acciones de clasificación predeterminadas.



Captura de pantalla 145: Estructura de carpeta raíz y subcarpetas

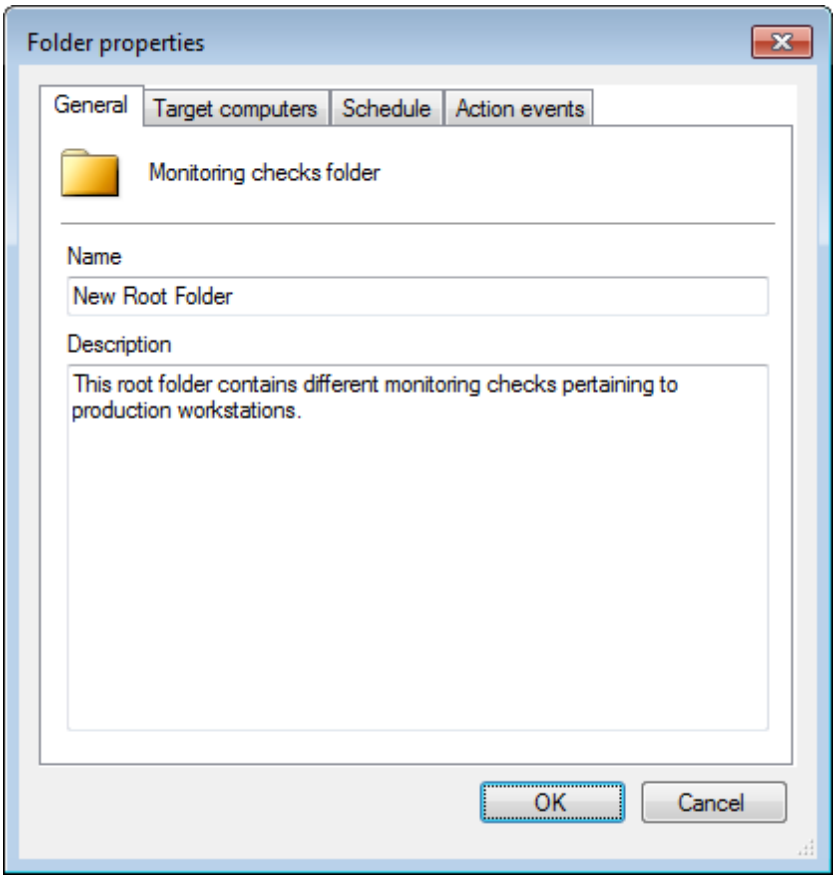
Las comprobaciones se organizan en carpetas raíz y subcarpetas. Los objetos heredan la configuración de la carpeta principal. Esto le permite configurar una serie de comprobaciones de supervisión de forma simultánea.

10.2 Crear y configurar una carpeta raíz

Una carpeta raíz es una carpeta principal que puede contener un conjunto de subcarpetas y supervisión activa. Cada uno de los objetos secundarios de una carpeta raíz hereda la misma configuración. Esto permite la configuración rápida de múltiples comprobaciones de supervisión y subcarpetas.

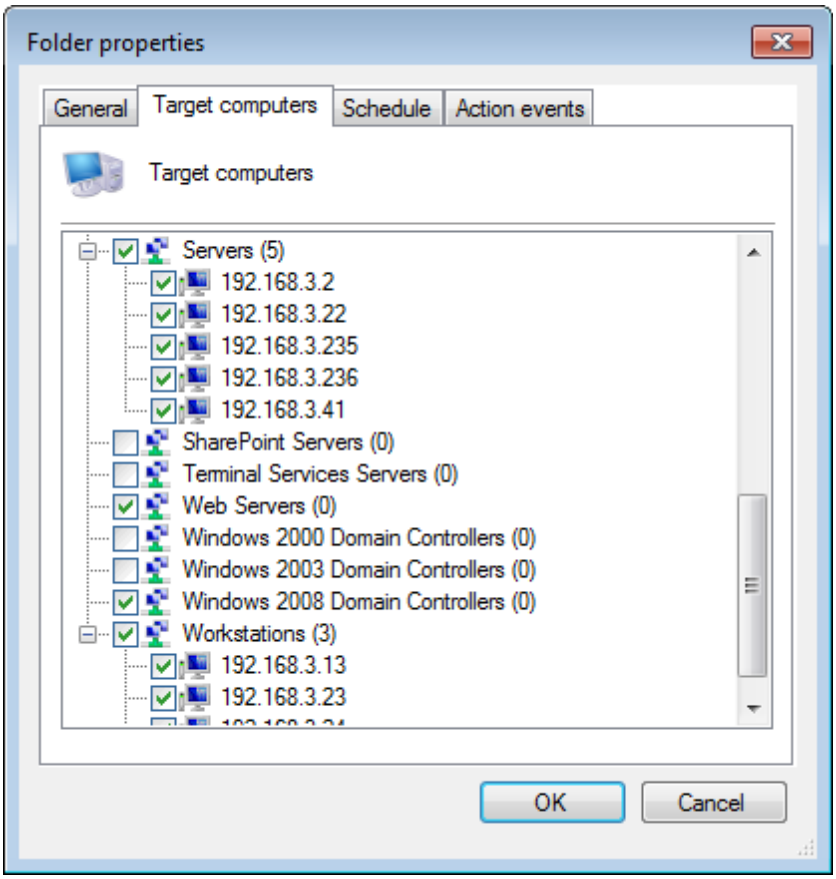
Para crear una nueva carpeta raíz:

1. En la ficha **Configuration > Active Monitoring > Common tasks**, haga clic en **Create root folder**. Se abre el cuadro de diálogo **Folder properties**.



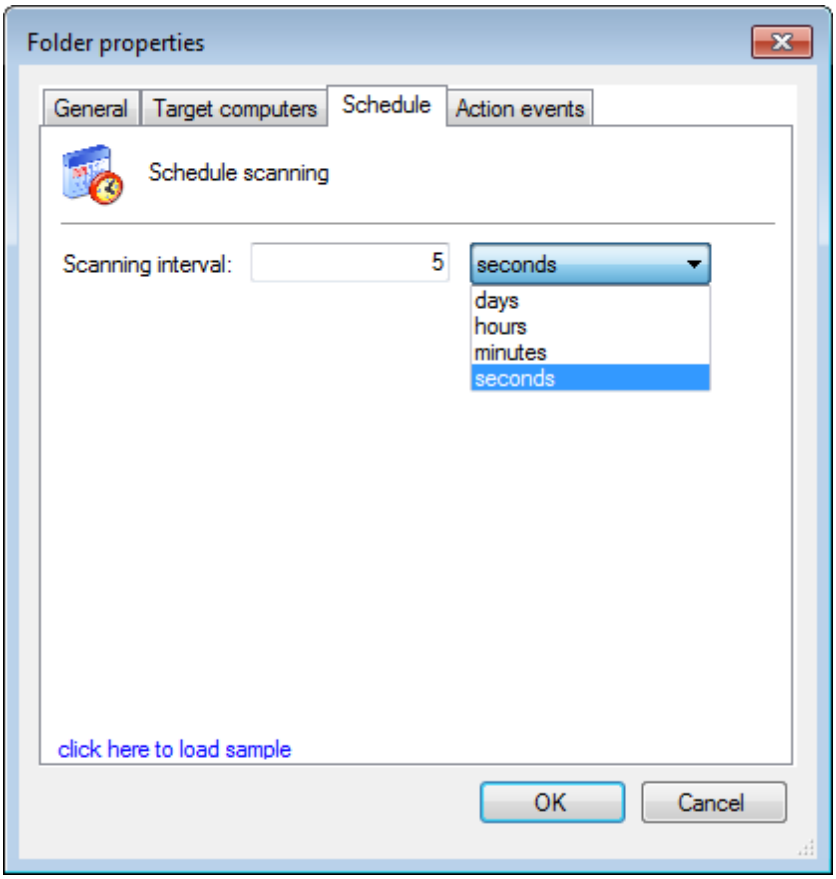
Captura de pantalla 146: Ficha Folder properties - General

2. Especifique un nombre y una descripción opcional en los campos **Name** y **Description**.



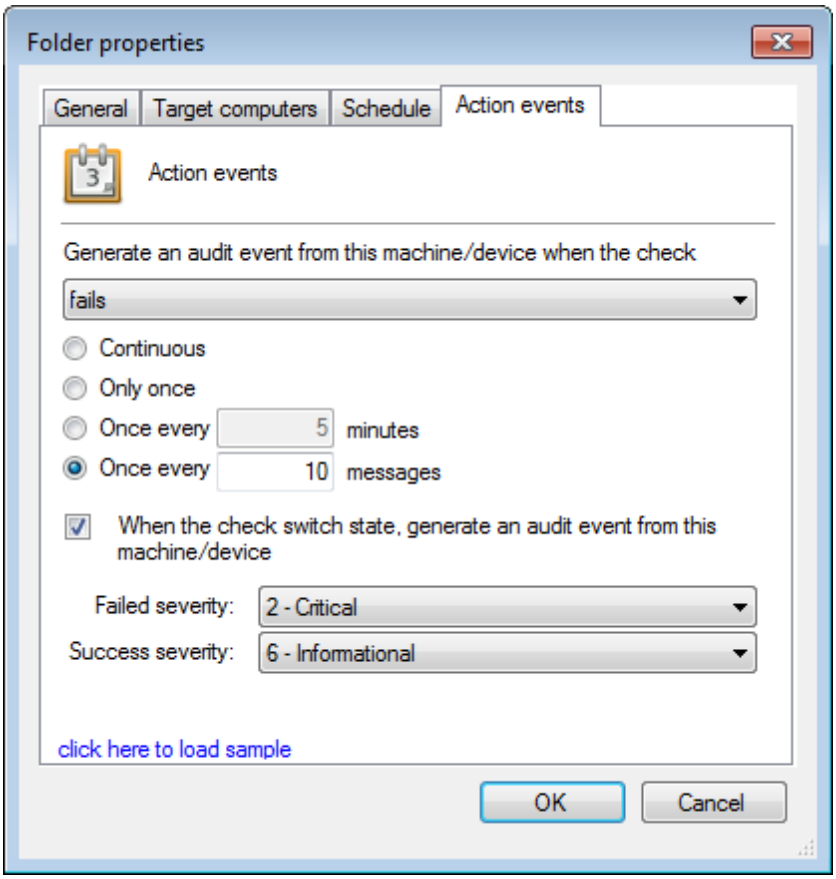
Captura de pantalla 147: Ficha Folder properties - Target computer

3. Haga clic en la ficha **Target computers** y seleccione los orígenes de eventos. La supervisión activa agregada a esta nueva carpeta se aplica a los orígenes de eventos seleccionados.



Captura de pantalla 148: Ficha Folder properties - Schedule

4. En la ficha **Schedule**, defina el intervalo de tiempo en el cual GFI EventsManager ejecuta las comprobaciones de supervisión en los orígenes de evento seleccionados. De forma predeterminada, el intervalo de comprobación de supervisión se define en 5 segundos.



Captura de pantalla 149: Ficha Folder Properties - Action events

> **Nota**
>
> Independientemente de si la supervisión activa falla o tiene éxito, el equipo que ejecuta la comprobación genera un registro de eventos. Este registro de eventos puede ser procesado por las reglas de procesamiento de eventos que permiten activar alertas o ejecutar secuencias de comando o aplicaciones para las operaciones de recuperación. Para obtener más información, consulte Crear nuevas reglas desde eventos existentes.

5. En la ficha **Action events**, configure cuándo se generan registros de eventos y cómo GFI EventsManager clasifica los eventos generados.
Las opciones disponibles se describen en la tabla siguiente:

Tabla 71: Comprobaciones de supervisión - Eventos de acción

Opción	Descripción
Generate an audit event from this machine/device when the check	GFI EventsManager le permite generar registros de eventos después de haber comprobado que no hay irregularidades en el origen de eventos. En el menú desplegable, seleccione: » **Fails**: permite generar un registro de eventos cuando falla la comprobación. » **Succeeds**: permite generar un registro de eventos cuando la comprobación se ejecuta correctamente. » **Fails or Succeeds**: permite generar un registro de eventos cada vez que se ejecuta la comprobación en los orígenes de eventos especificados.
Continuous	Genera un registro de eventos cada vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.

Opción	Descripción
Only once	Genera un registro de eventos la primera vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.
Once every {X} minutes	Genera un registro de eventos cada vez que transcurre la cantidad de minutos que usted especificó.
Once every {X} messages	Genera un registro de eventos cada vez que se alcanza la cantidad de mensajes que usted especificó. Por ejemplo: si escribe 10, solamente se genera un evento después de ejecutar 10 veces la comprobación de forma correcta/incorrecta/ambas situaciones.
When the check switch state, generate an audit event from this machine/device	Genera un registro de eventos cuando el control cambia del estado Fail a Succeed o viceversa.
Failed severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación fallida del sistema.
Success severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación del sistema exitosa.

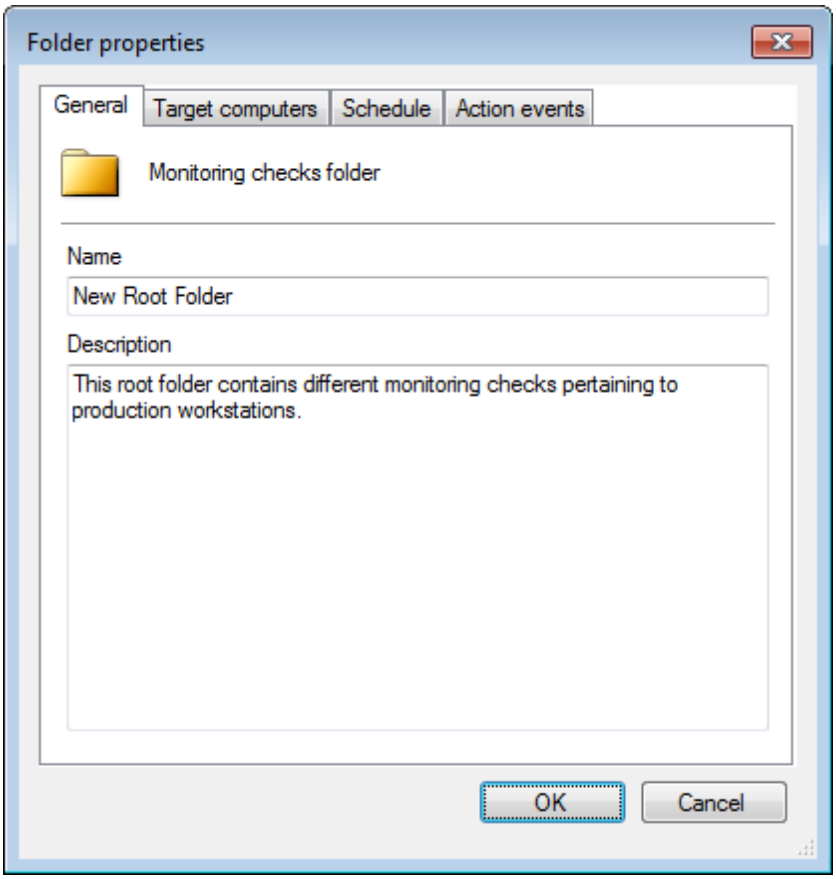
6. Haga clic en **OK** para aceptar.

10.3 Agregar subcarpetas a una carpeta raíz

Las subcarpetas se usan para subdividir un grupo de comprobaciones de supervisión que comparten algunas características comunes, pero pueden (por ejemplo) destinarse a diferentes tipos de orígenes de eventos.

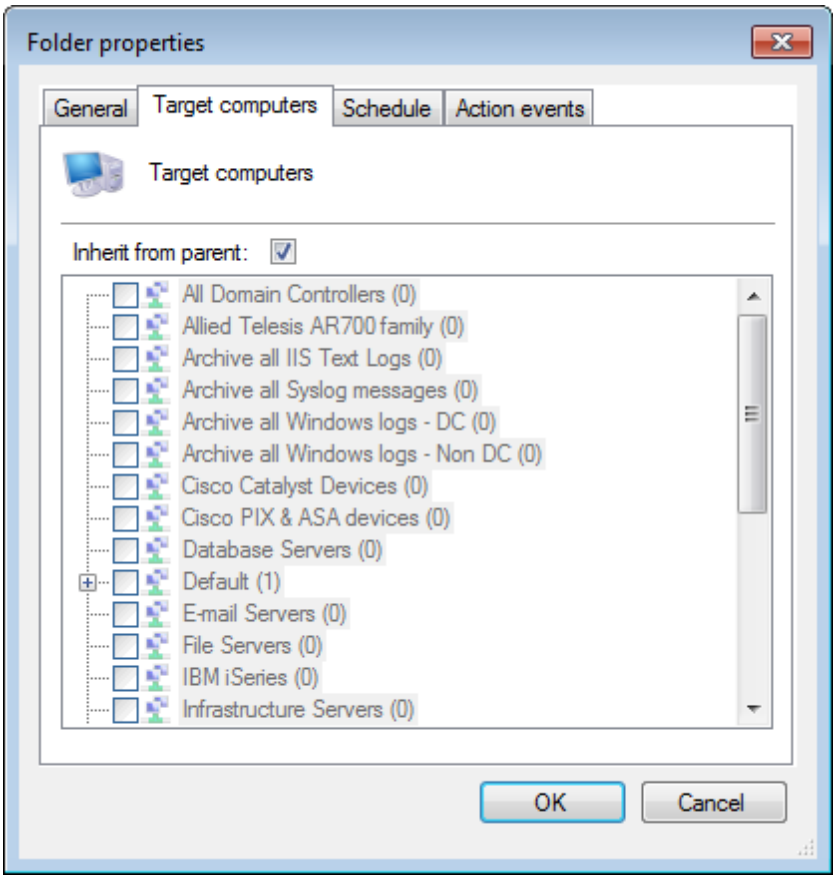
Para agregar una subcarpeta nueva:

1. En **Configuration > Active Monitoring > Monitoring checks**, haga clic con el botón secundario en una carpeta raíz/subcarpeta y seleccione **Create new folder**.



Captura de pantalla 150: Ficha Folder properties - General

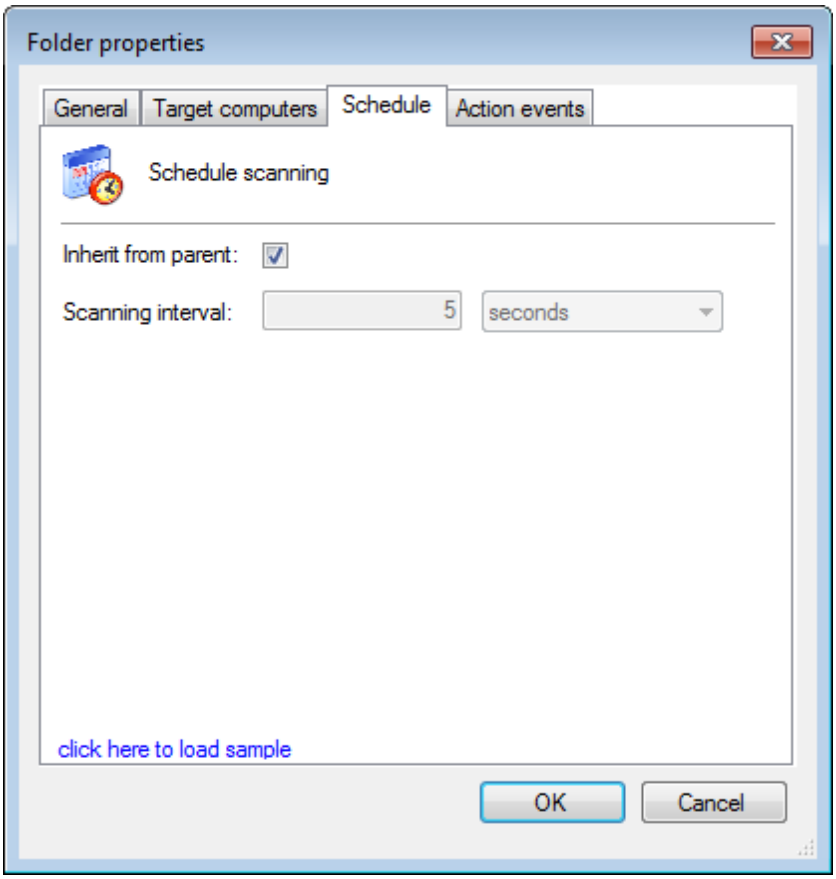
2. En la ficha **General**, escriba el nombre de la nueva carpeta y una descripción opcional.



Captura de pantalla 151: Ficha Folder properties - Target computer

> **Nota**
>
> Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

3. Haga clic en la ficha **Target computers** y seleccione los orígenes de eventos. Las supervisiones activas que se agregan a esta nueva carpeta se aplican a los orígenes de eventos seleccionados.

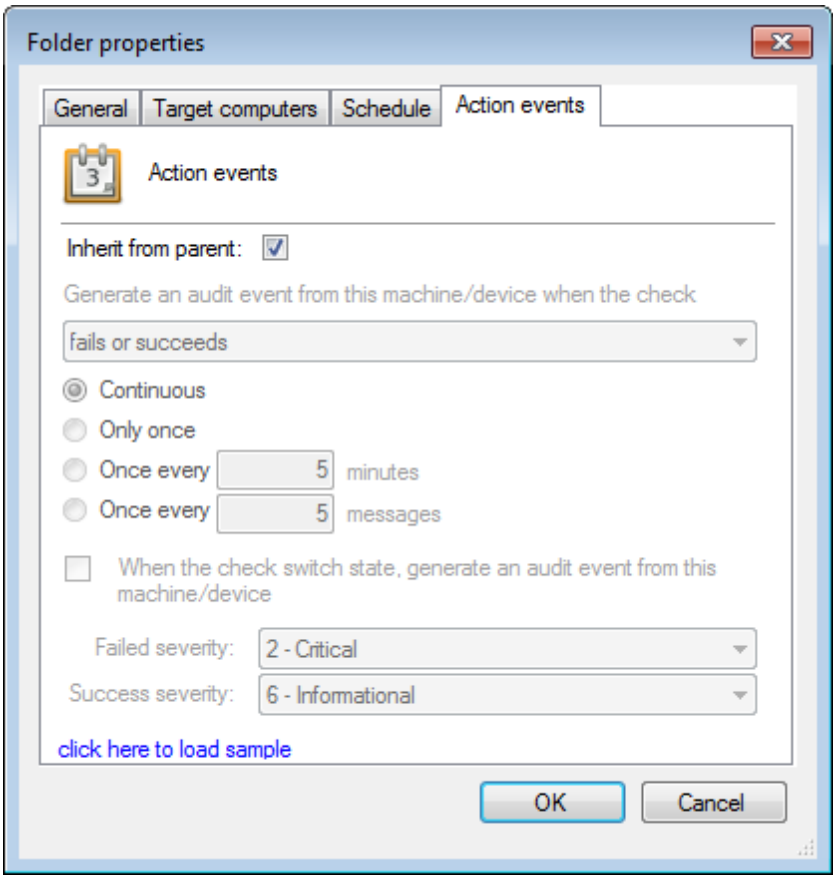


Captura de pantalla 152: Ficha Folder properties - Schedule

Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

4. En la ficha **Schedule**, establezca el intervalo en el que GFI EventsManager ejecuta las comprobaciones de supervisión en los orígenes de eventos seleccionados. De forma predeterminada, el intervalo de comprobación de supervisión se define en 5 segundos.



Captura de pantalla 153: Ficha Folder Properties - Action events

Nota

Independientemente de si la supervisión activa falla o tiene éxito, el equipo que ejecuta la comprobación genera un registro de eventos. Este registro de eventos puede ser procesado por las reglas de procesamiento de eventos que permiten activar alertas o ejecutar secuencias de comando o aplicaciones para las operaciones de recuperación. Para obtener más información, consulte Crear nuevas reglas desde eventos existentes.

Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

5. En la ficha **Action events**, configure cuándo se generan registros de eventos y cómo GFI EventsManager clasifica los eventos generados.
Las opciones disponibles se describen en la tabla siguiente:

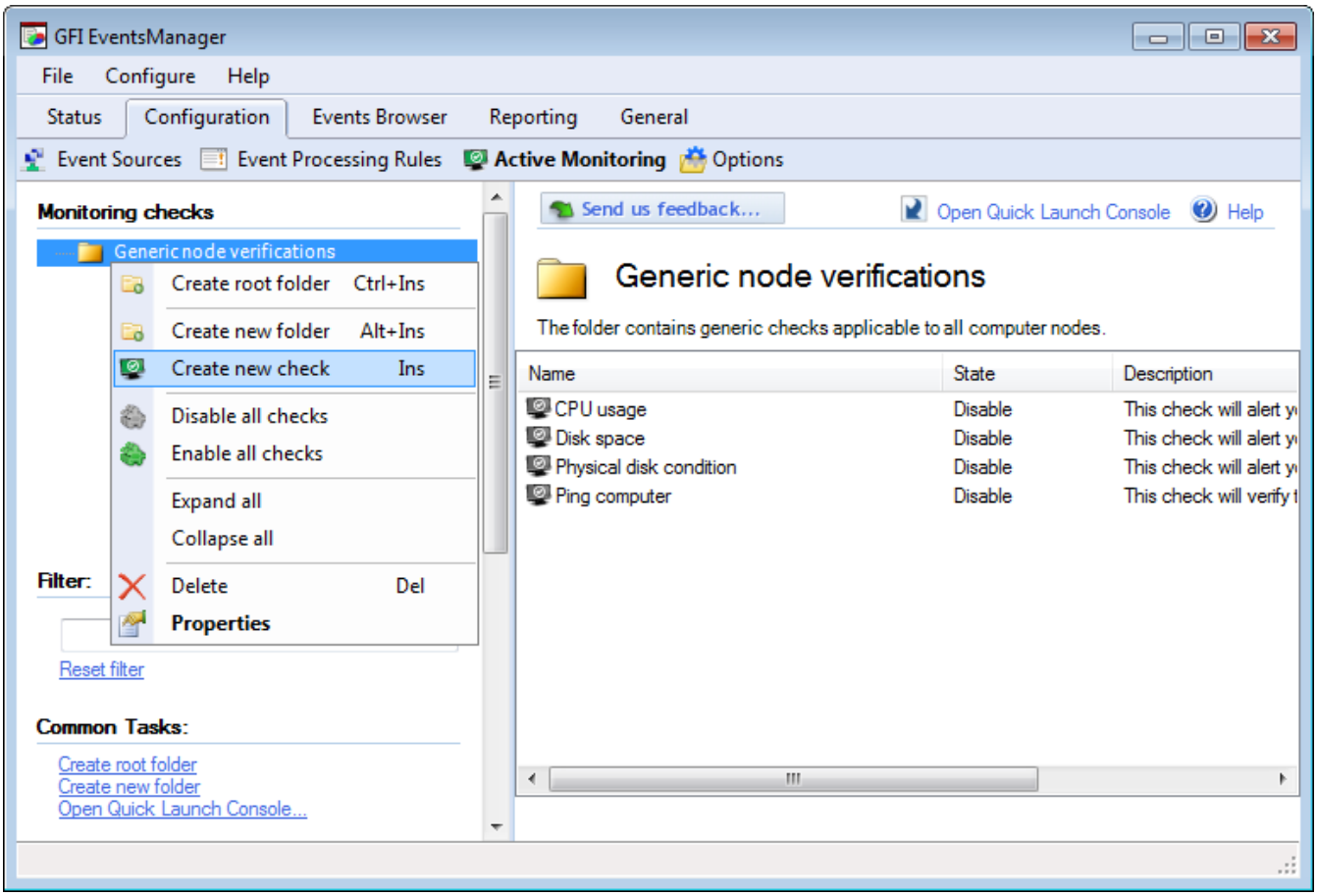
Tabla 72: Comprobaciones de supervisión - Eventos de acción

Opción	Descripción
Generate an audit event from this machine/device when the check	GFI EventsManager le permite generar registros de eventos después de haber comprobado que no hay irregularidades en el origen de eventos. En el menú desplegable, seleccione: » **Fails**: permite generar un registro de eventos cuando falla la comprobación. » **Succeeds**: permite generar un registro de eventos cuando la comprobación se ejecuta correctamente. » **Fails or Succeeds**: permite generar un registro de eventos cada vez que se ejecuta la comprobación en los orígenes de eventos especificados.
Continuous	Genera un registro de eventos cada vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.
Only once	Genera un registro de eventos la primera vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.
Once every {X} minutes	Genera un registro de eventos cada vez que transcurre la cantidad de minutos que usted especificó.
Once every {X} messages	Genera un registro de eventos cada vez que se alcanza la cantidad de mensajes que usted especificó. Por ejemplo: si escribe 10, solamente se genera un evento después de ejecutar 10 veces la comprobación de forma correcta/incorrecta/ambas situaciones.
When the check switch state, generate an audit event from this machine/device	Genera un registro de eventos cuando el control cambia del estado Fail a Succeed o viceversa.
Failed severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación fallida del sistema.
Success severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación del sistema exitosa.

6. Haga clic en **OK** para aceptar.

10.4 Crear y configurar comprobaciones de supervisión activa

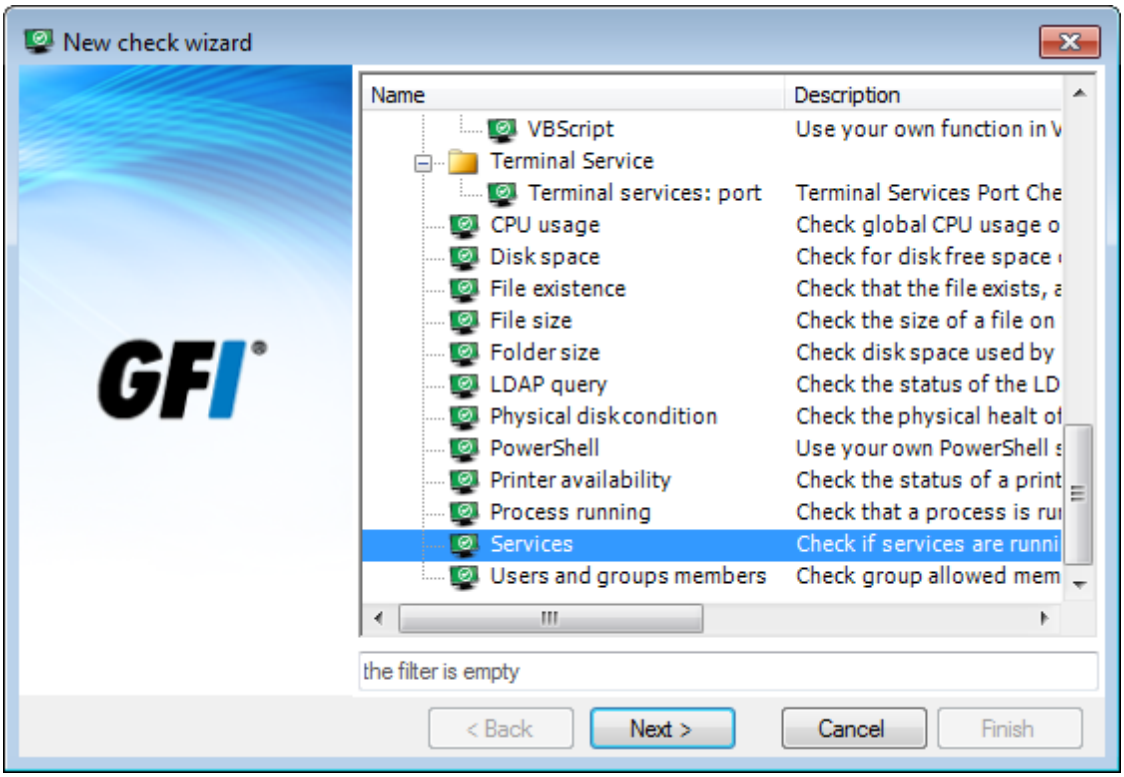
Para crear una nueva comprobación de supervisión activa:



Captura de pantalla 154: Crear una nueva comprobación de supervisión activa

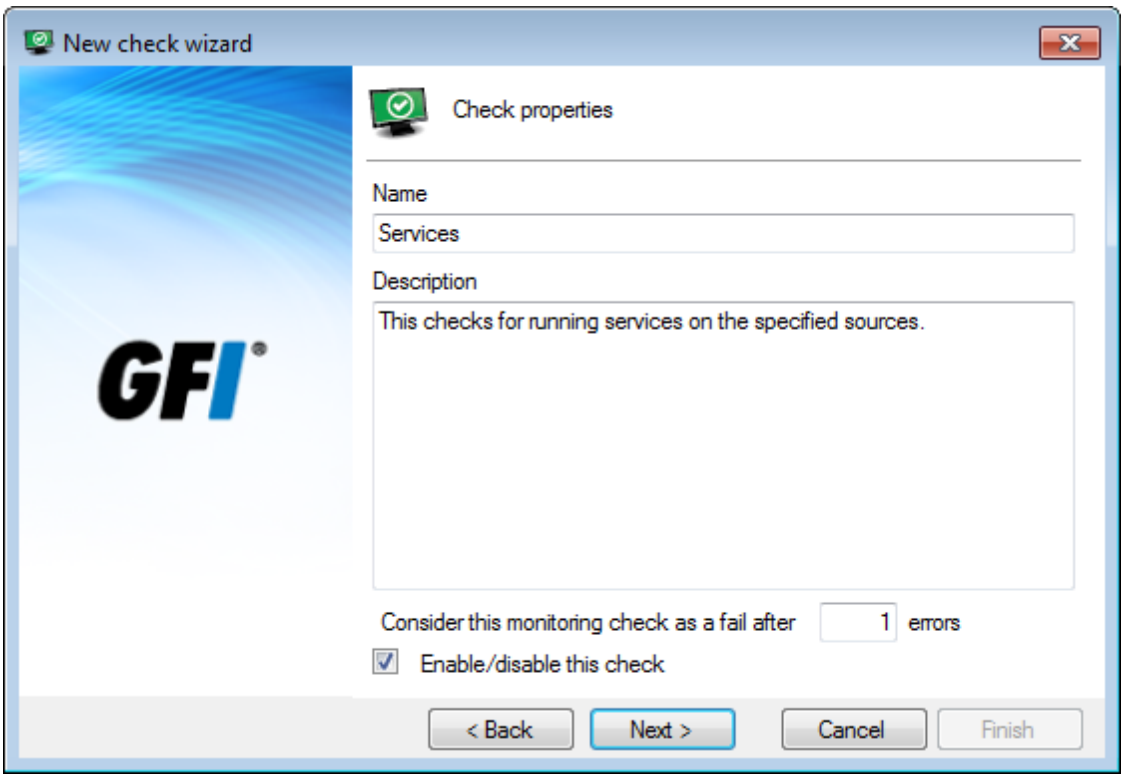
1. Haga clic en **Configuration > Active Monitoring.**

2. Haga clic con el botón secundario en la raíz/subcarpeta donde desea guardar la nueva comprobación de supervisión y seleccione **Create new check**.



Captura de pantalla 155: Seleccionar tipo de comprobación

3. Seleccione el tipo de comprobación y haga clic en **Next**.

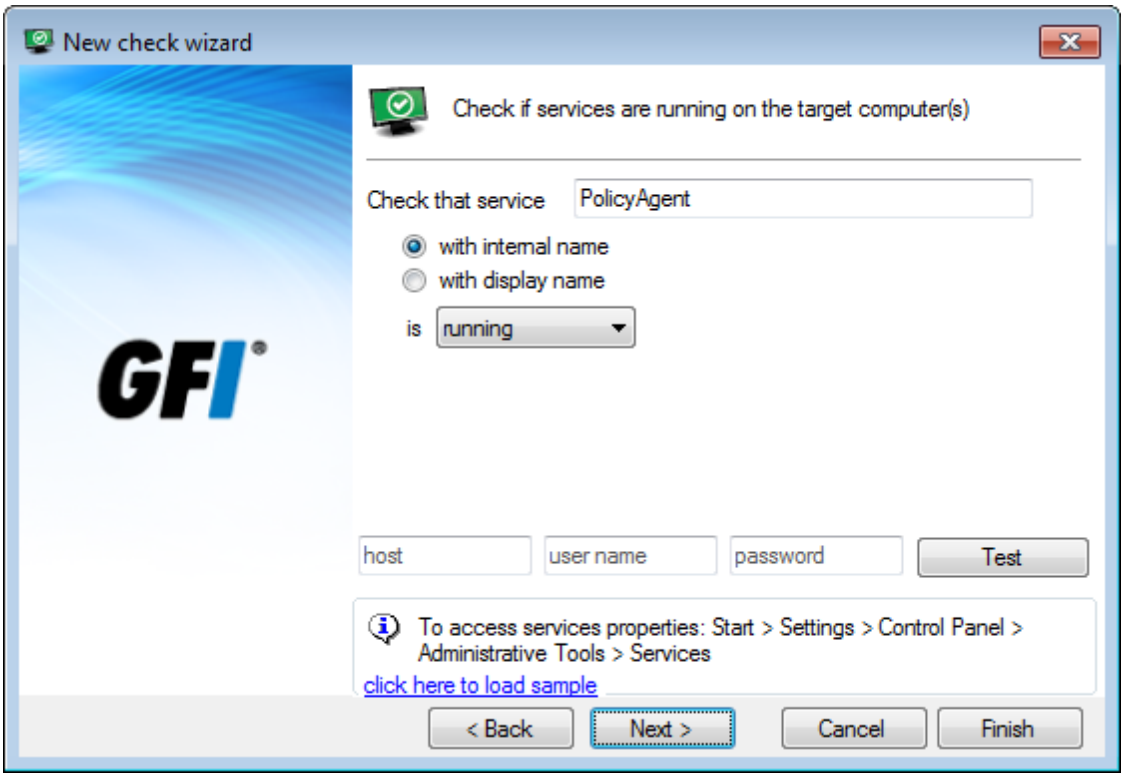


Captura de pantalla 156: Configurar propiedades generales de comprobación

4. Especifique un nombre y una descripción opcional en los campos **Name** y **Description**.

5. En el cuadro de texto **Consider this monitoring check as fail after {X} errors**, especifique el número de errores que deben ocurrir antes de que las nuevas comprobaciones se clasifiquen como **Failed** o erróneas.

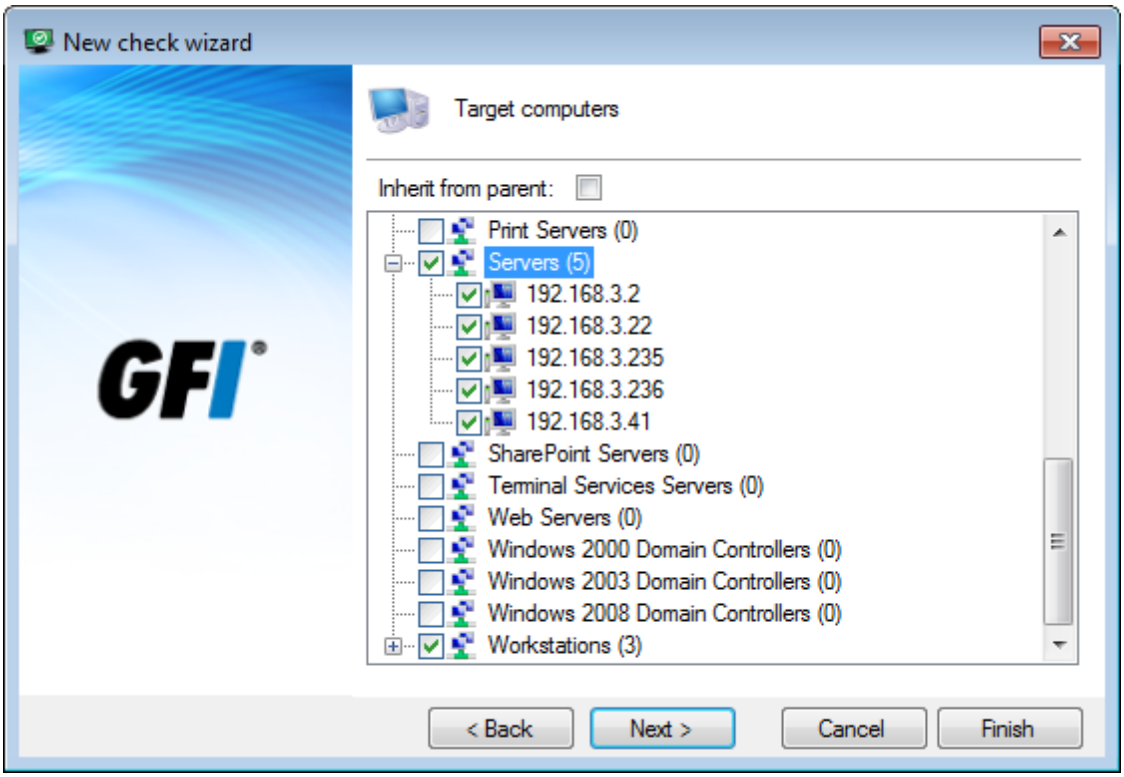
6. Marque o desmarque **Enable/disable this check** para activar/desactivar la nueva comprobación de supervisión. Haga clic en **Siguiente**.



Captura de pantalla 157: Configurar parámetros de comprobación de supervisión

7. Configure los parámetros que se deben comprobar y haga clic en **Next**.

> **Nota**
>
> Este paso es diferente para cada tipo de comprobación que usted seleccione en el Paso 3.

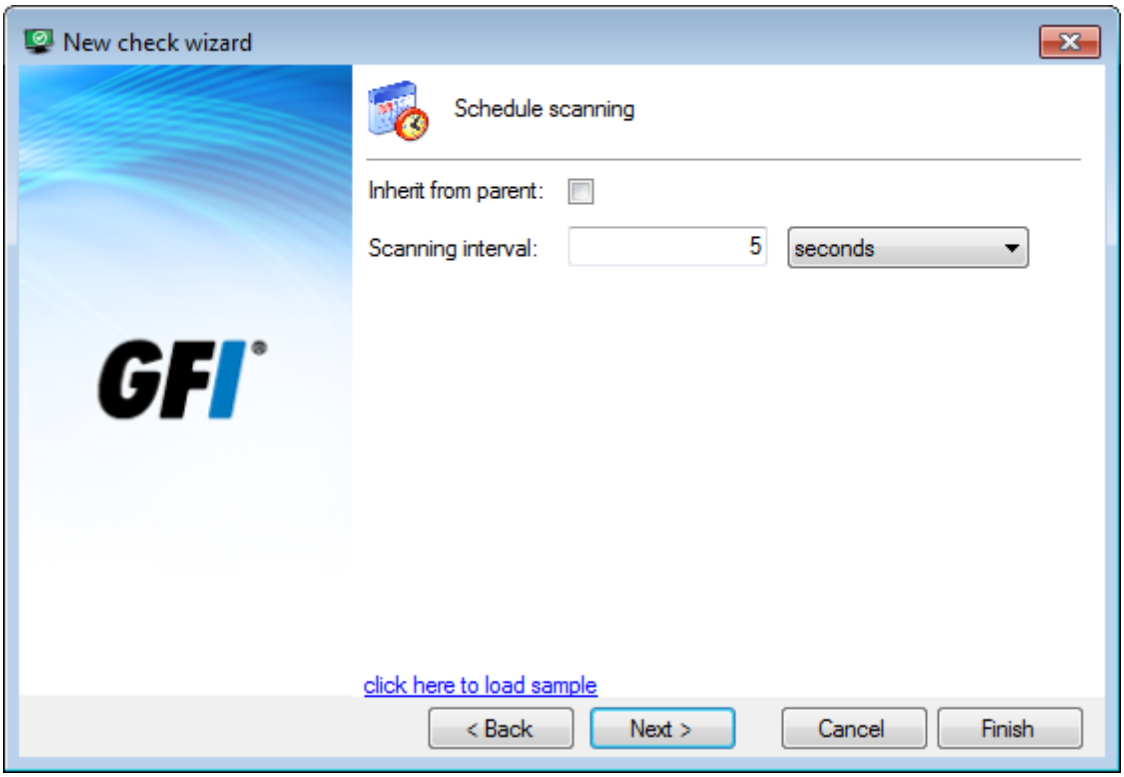


Captura de pantalla 158: Seleccionar orígenes efectuados

Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

8. En la lista de orígenes de eventos, seleccione los equipos que desea supervisar con esta nueva comprobación. Haga clic en **Siguiente**.

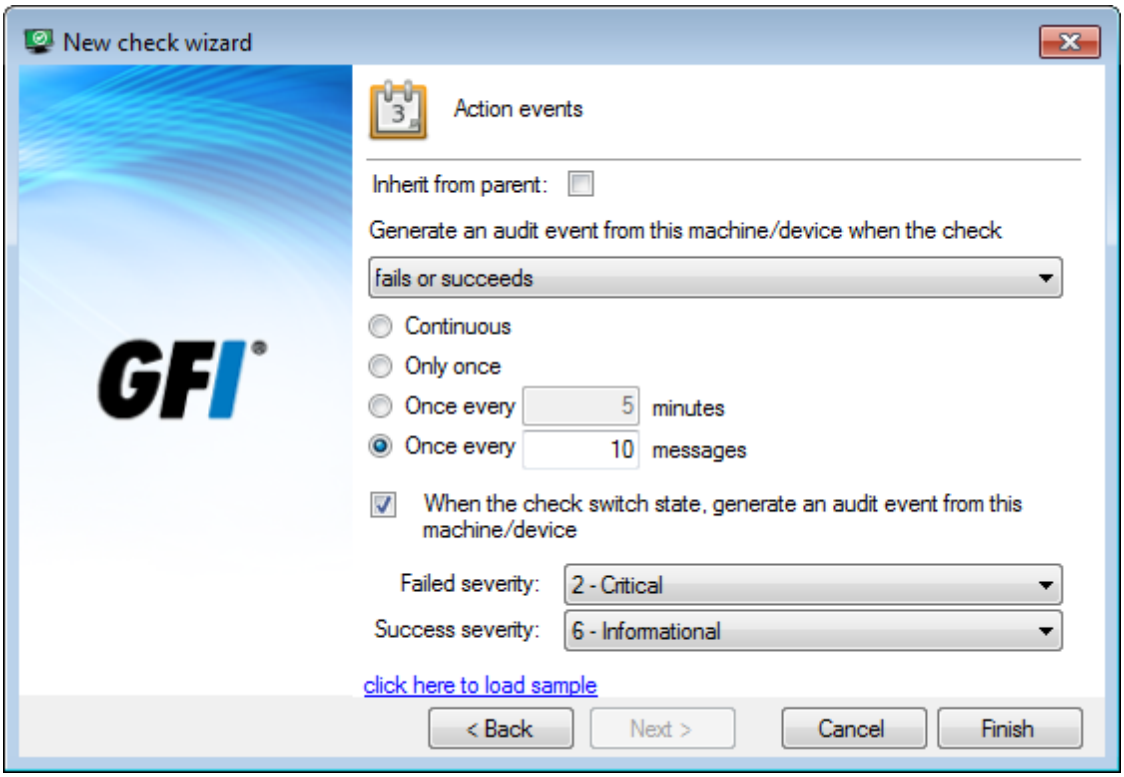


Captura de pantalla 159: Definir el intervalo de tiempo del análisis

Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

9. Configure el programa de intervalo del análisis para la nueva comprobación. De forma predeterminada, la comprobación analiza los orígenes seleccionados una vez cada 5 segundos.



Captura de pantalla 160: Configurar acciones de registro de eventos

Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

10. Una comprobación de supervisión genera un registro de eventos independientemente de si tiene éxito o falla. En **Action events**, cuándo se generan los registros de eventos y cómo GFI EventsManager clasifica los registros generados.
Las opciones disponibles se describen en la tabla siguiente:

Tabla 73: Comprobaciones de supervisión - Eventos de acción

Opción	Descripción
Generate an audit event from this machine/device when the check	GFI EventsManager le permite generar registros de eventos después de haber comprobado que no hay irregularidades en el origen de eventos. En el menú desplegable, seleccione: » **Fails**: permite generar un registro de eventos cuando falla la comprobación. » **Succeeds**: permite generar un registro de eventos cuando la comprobación se ejecuta correctamente. » **Fails or Succeeds**: permite generar un registro de eventos cada vez que se ejecuta la comprobación en los orígenes de eventos especificados.
Continuous	Genera un registro de eventos cada vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.
Only once	Genera un registro de eventos la primera vez que la comprobación se ejecuta correctamente/incorrectamente/ambas situaciones.
Once every {X} minutes	Genera un registro de eventos cada vez que transcurre la cantidad de minutos que usted especificó.

Opción	Descripción
Once every {X} messages	Genera un registro de eventos cada vez que se alcanza la cantidad de mensajes que usted especificó. Por ejemplo: si escribe 10, solamente se genera un evento después de ejecutar 10 veces la comprobación de forma correcta/incorrecta/ambas situaciones.
When the check switch state, generate an audit event from this machine/device	Genera un registro de eventos cuando el control cambia del estado Fail a Succeed o viceversa.
Failed severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación fallida del sistema.
Success severity	Seleccione el nivel de gravedad que GFI EventsManager asigna al registro de eventos de una comprobación del sistema exitosa.

11. Haga clic en **Finish** para finalizar.

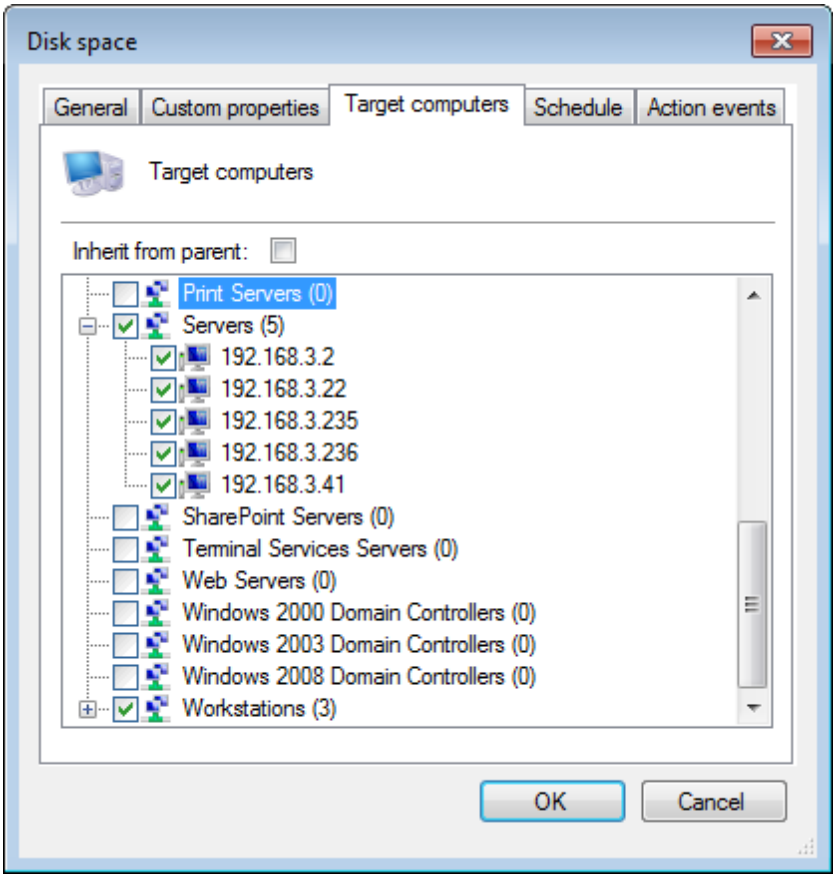
10.5 Aplicar comprobaciones de supervisión activa

La supervisión activa se puede aplicar a orígenes de eventos individuales o grupos de orígenes de eventos. Los orígenes de eventos se pueden seleccionar a nivel de comprobación por comprobación o a nivel de la carpeta raíz. Configurar los parámetros a nivel de la carpeta permite que las comprobaciones relativas hereden la misma configuración de orígenes de eventos.

Para asignar una comprobación de supervisión preconfigurada:

1. Acceda a **Configuration > Active Monitoring**.

2. Haga clic con el botón secundario en la supervisión activa/carpeta que desea asignar a sus orígenes de eventos y seleccione **Properties**.



Captura de pantalla 161: Ficha Target computers

3. En la ficha **Target computers**, seleccione el origen de evento o grupo de orígenes de eventos.

4. Haga clic en **OK** para aceptar.

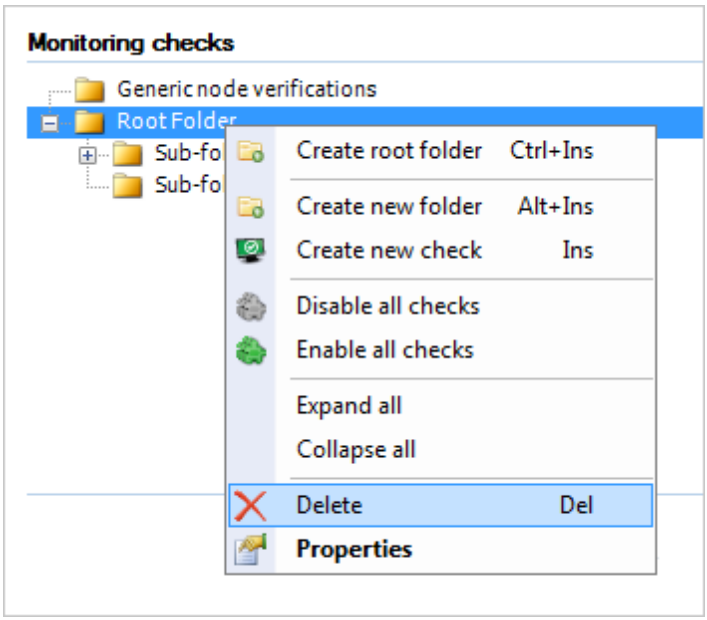
Nota

Seleccione **Inherit from parent** para usar la misma configuración que la carpeta principal.

10.6 Eliminar carpetas y comprobaciones de supervisión

Para eliminar una carpeta/comprobación de supervisión:

1. Acceda a **Configuration > Active Monitoring**.



Captura de pantalla 162: Eliminar carpetas y comprobaciones de supervisión

2. En la sección **Monitoring checks**, haga clic con el botón secundario en la carpeta/comprobación de supervisión que desea eliminar y seleccione **Delete**.

Importante

Al eliminar una carpeta raíz (carpeta principal), también se elimina todo el contenido. Asegúrese de eliminar solamente los elementos no deseados.

11 Alertas y acciones predeterminadas

En este capítulo, se proporciona información acerca de los métodos de alerta disponibles y acerca de cómo configurar cada uno de ellos de acuerdo con sus necesidades. Durante el procesamiento de eventos, GFI EventsManager ejecuta de forma automática las acciones y activa alertas cuando se producen determinados eventos.

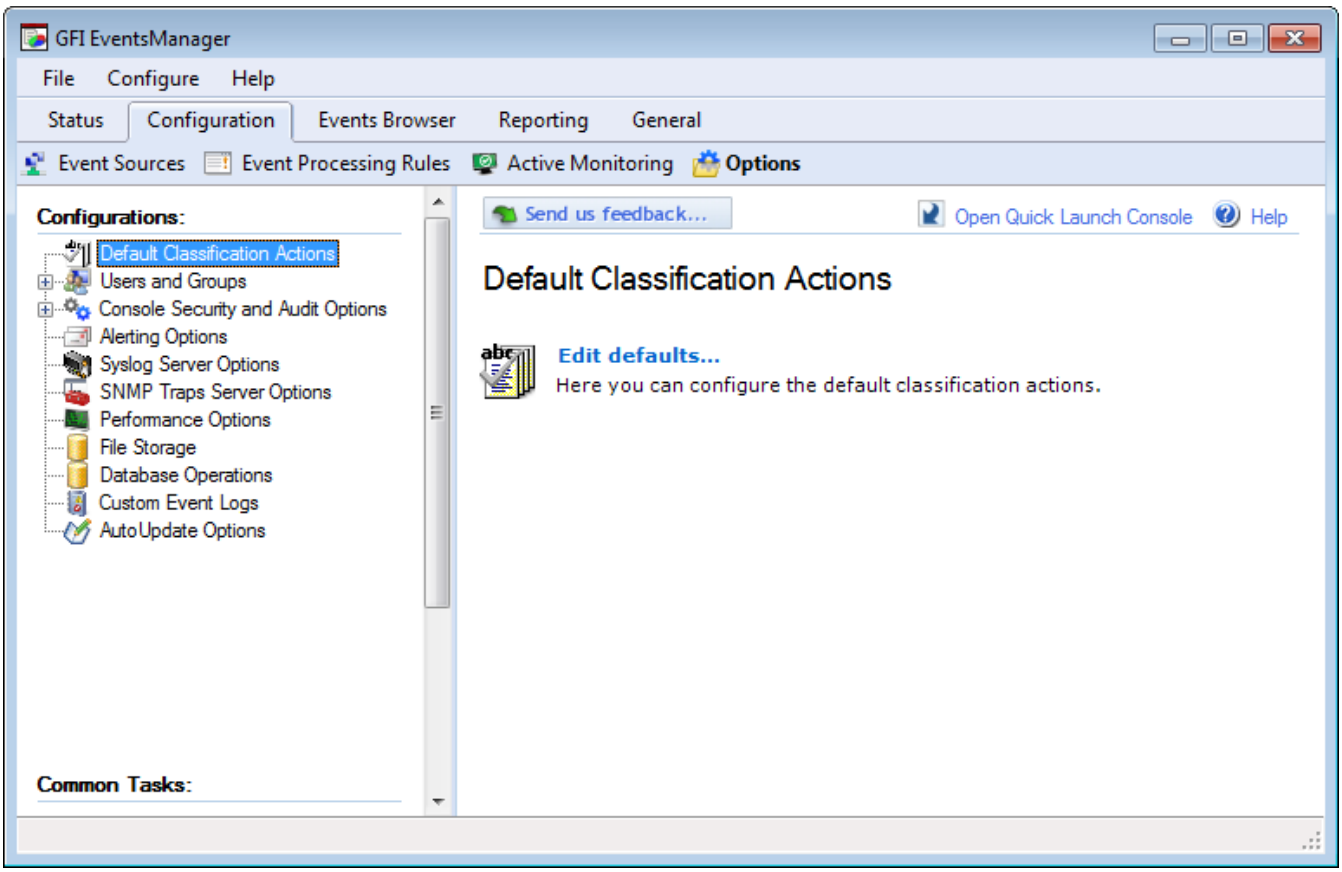
Temas de este capítulo:

11.1 Configurar acciones de clasificación predeterminadas 216

11.2 Configurar opciones de alerta 218

11.1 Configurar acciones de clasificación predeterminadas

A través de los parámetros de configuración especificados en las acciones de clasificación predeterminadas, puede activar alertas y acciones que se basen solamente en la clasificación del evento. Por ejemplo: los parámetros de clasificación predeterminados se pueden configurar para activar alertas por correo electrónico cuando se produce cualquier tipo de evento (crítico, alto, medio y bajo), pero solamente para archivar los eventos críticos.

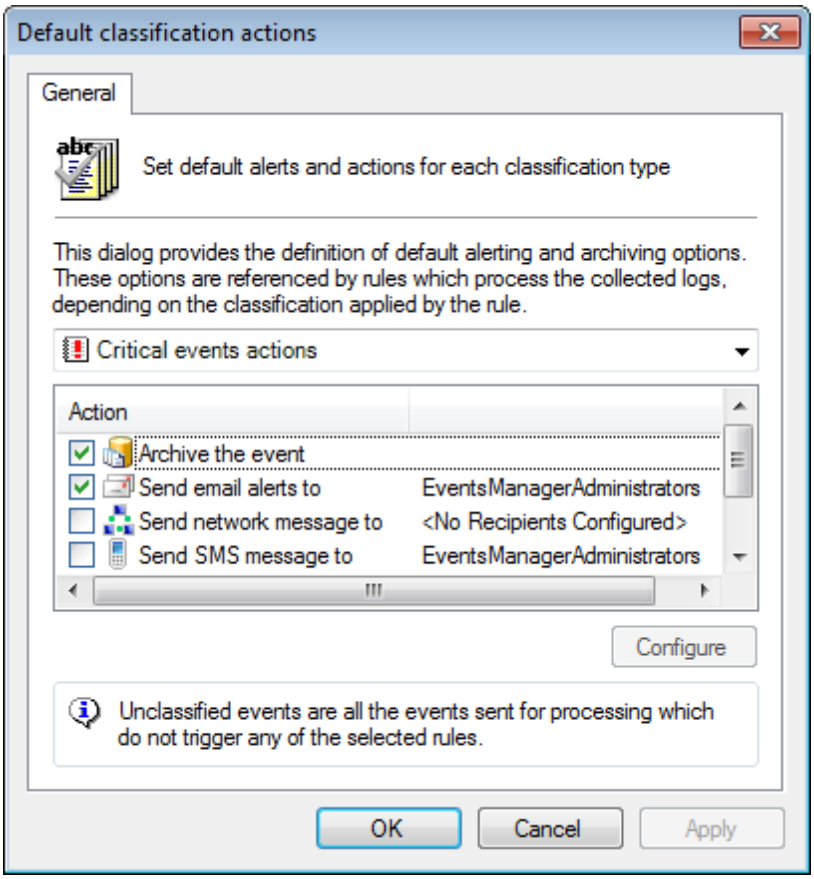


de alguna bases de datos.

Captura de pantalla 163: Configurar acciones de clasificación predeterminadas

Para configurar acciones de clasificación predeterminadas:

1. En la ficha **Configuration > Options**, haga clic con el botón secundario en el nodo **Default Classification Actions** y en **Edit defaults…**.


Default classification actions
General
Set default alerts and actions for each classification type
This dialog provides the definition of default alerting and archiving options. These options are referenced by rules which process the collected logs, depending on the classification applied by the rule.
Critical events actions
Action
Archive the event
Send email alerts to
EventsManagerAdministrators
Send network message to
<No Recipients Configured>
Send SMS message to
EventsManagerAdministrators
Configure
Unclassified events are all the events sent for processing which do not trigger any of the selected rules.
OK
Cancel
Apply

Captura de pantalla 164: Cuadro de diálogo Default Classification Actions

2. En el menú desplegable, seleccione la clasificación de evento que desea configurar.

3. En la lista **Action**, seleccione las acciones que se deben activar y haga clic en **Configure**. Las acciones disponibles son:

Tabla 74: Acciones de clasificación predeterminadas

Acción	Descripción
Archive the event	Permite archivar los eventos sin procesamiento adicional.
Send email alerts to	Haga clic en **Configure** y seleccione los destinatarios. **NOTA** Asegúrese de que los usuarios tengan configurada una dirección de correo electrónico válida. Para obtener más información, consulte Administrar cuentas de usuario.
Send network messages to	Haga clic en **Configure** y seleccione los destinatarios. **NOTA** Asegúrese de que los usuarios tengan configurado un nombre de equipo/IP válido. Para obtener más información, consulte Administrar cuentas de usuario.
Send SMS message to	Haga clic en **Configure** y seleccione los destinatarios. **NOTA** Asegúrese de que los usuarios tengan configurado un número de celular válido. Para obtener más información, consulte Administrar cuentas de usuario.

Acción	Descripción
Run file	Haga clic en **Configure** y seleccione el archivo que desea ejecutar y especifique los parámetros de línea de comandos que desea pasar al archivo. Entre los archivos admitidos se incluyen: » Secuencias de comando VB: *.VBS » Archivos por lotes: *.BAT » Ejecutables: *.EXE
Send SNMP Message	Haga clic en **Configure** y seleccione los destinatarios.
Scan computer	GFI EventsManager vuelve a auditar el equipo.
Run checks on computer	Haga clic en **Configure** y seleccione las comprobaciones de supervisión que desee ejecutar cuando se desencadena la acción. **Nota** La supervisión activa se aplica a los orígenes de eventos correspondientes, seleccionados de la ficha Target computers. Para obtener más información, consulte Crear y configurar comprobaciones de supervisión activa. **Nota** Asegúrese de que el procesamiento de las comprobaciones de supervisión esté habilitado; de lo contrario, se descartarán las comprobaciones. Para obtener más información, consulte Configurar supervisión de orígenes de eventos.

4. Haga clic en **Apply** y **OK**.

Nota

La ejecución de acciones predeterminadas en eventos clasificados como **Low** puede generar una gran cantidad de tráfico de red cuando estén activadas las alertas por correo electrónico, SMS, red o SNMP. Esto también puede ser un problema cuando el archivado esté activado en eventos de baja importancia.

11.2 Configurar opciones de alerta

Las opciones de alerta le permiten configurar qué alertas se activan cuando se presenta un evento en particular. Por ejemplo, se puede configurar GFI EventsManager para que envíe alertas por correo electrónico y SMS a uno o más destinatarios cuando se procesa un evento **crítico**.

Esta sección contiene información acerca de:

» Configurar alertas por correo electrónico

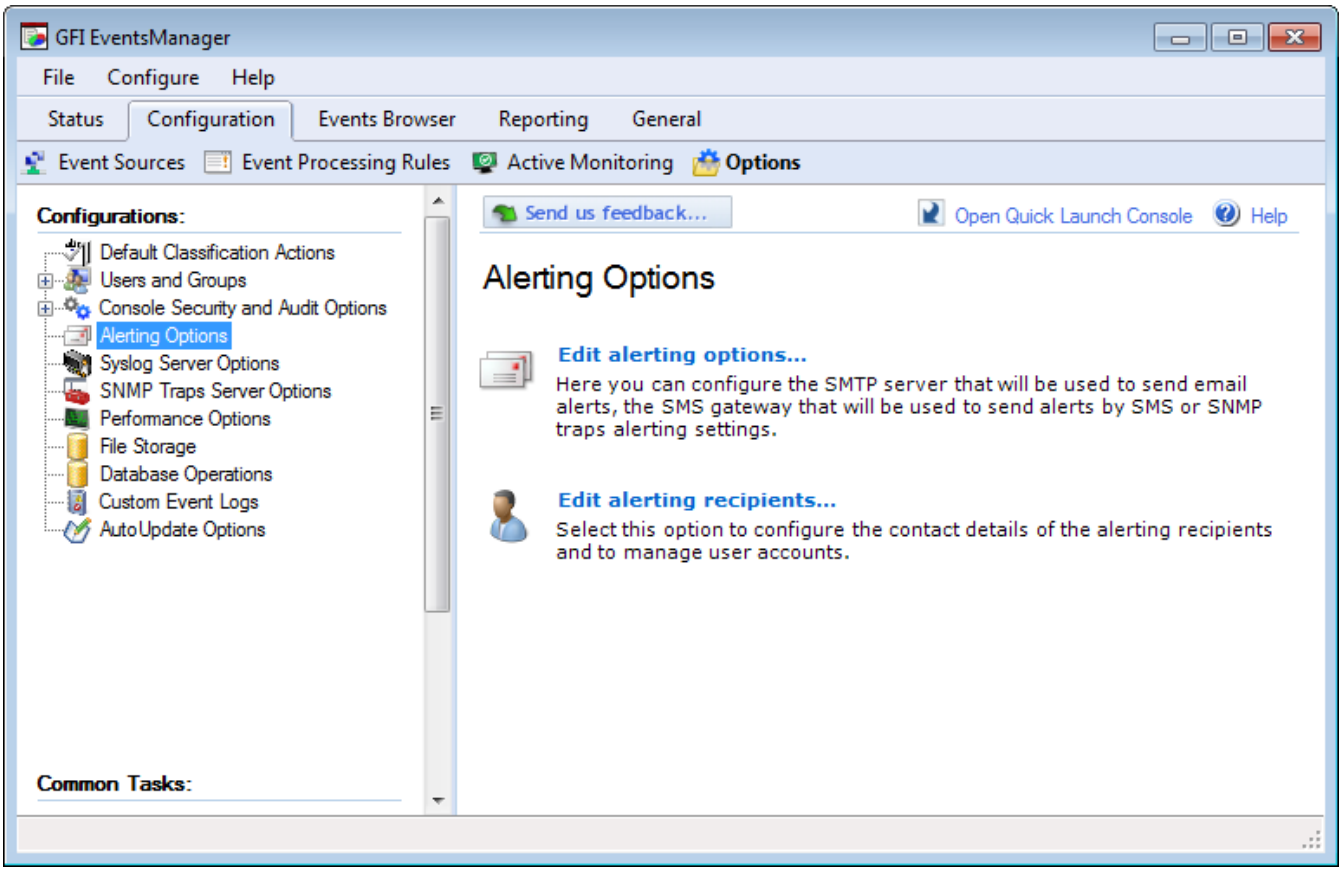
» Configurar alertas a través de la red

» Configurar alertas por SMS

» Configurar alertas a través de capturas SNMP

» Configurar parámetros generales

Para configurar opciones de alerta:



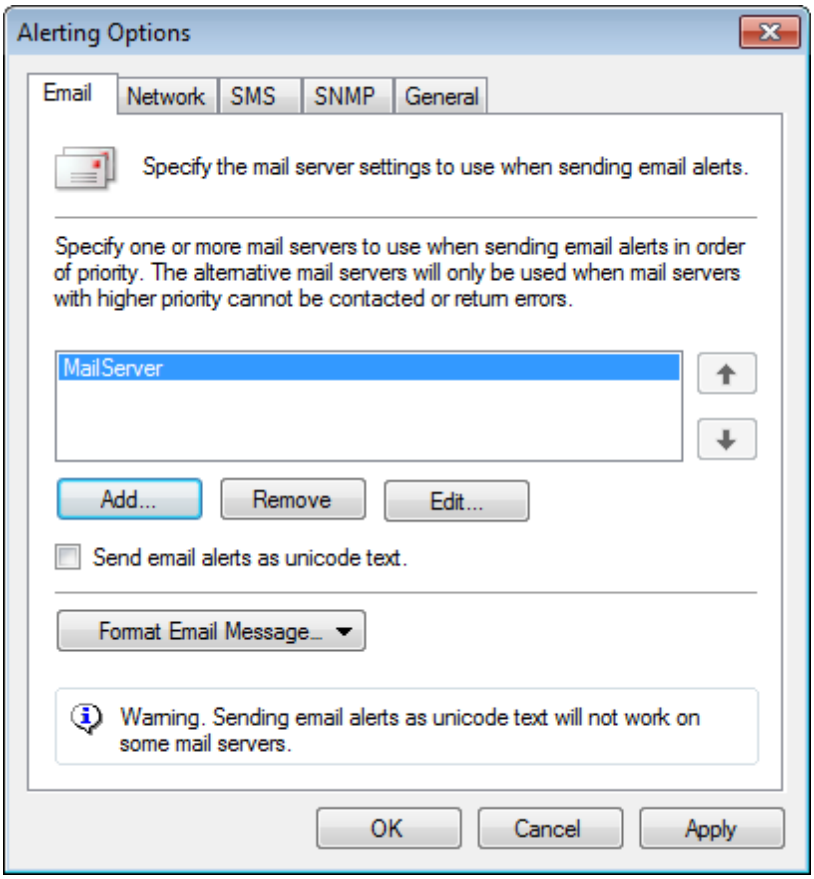
Captura de pantalla 165: Configurar opciones de alerta

1. Haga clic en la ficha **Configuration > Options**, haga clic con el botón secundario en **Alerting Options** y seleccione **Edit alerting options...**.

> **Nota**
>
> Seleccione Edit alert recipients para configurar los detalles de contacto de los destinatarios de la alerta y para administrar las cuentas de usuario. Para obtener más información, consulte Administrar cuentas de usuario.

2. Configure el método de alerta de su elección. Las siguientes secciones describen cómo configurar:

11.2.1 Alertas por correo electrónico


Alerting Options
Email
Network
SMS
SNMP
General
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
MailServer
Add...
Remove
Edit...
Send email alerts as unicode text.
Format Email Message...
Warning. Sending email alerts as unicode text will not work on some mail servers.
OK
Cancel
Apply

Captura de pantalla 166: Configurar opciones de correo electrónico

Para configurar alertas por correo electrónico:

1. En el cuadro de diálogo Alerting Options, haga clic en la ficha **Email**.

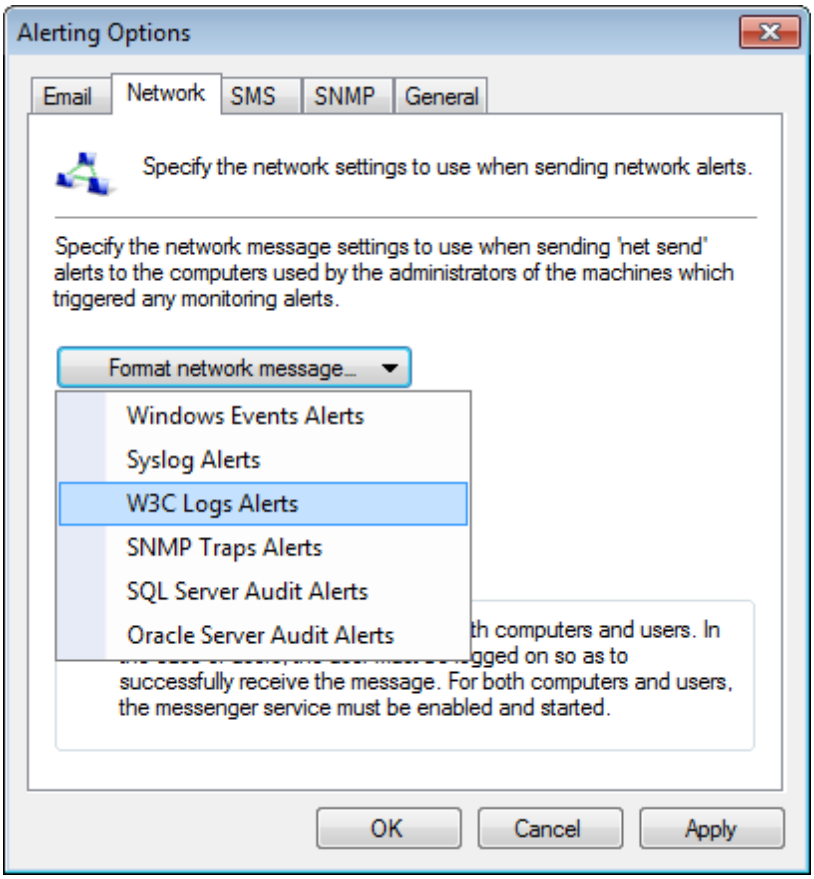
2. Configure las opciones que se describen a continuación:

Tabla 75: Cuadro de diálogo Alerting Options - Email alerts

Opción	Descripción
Add/Remove/Edit	Haga clic en **Add...** para especificar los detalles del servidor de correo, incluido el nombre del servidor/IP, las credenciales de inicio de sesión y la dirección de correo electrónico del destinatario. Use el botón **Remove** o **Edit** para eliminar un servidor seleccionado o editar los detalles, respectivamente.
Teclas de flechas hacia arriba/hacia abajo	Utilice las teclas de flecha para cambiar la posición del servidor de correo seleccionado. GFI EventsManager intenta enviar alertas de correo electrónico a través del primer servidor de correo. Si no tiene éxito, se comprueban de forma recursiva los siguientes servidores de correo.
Send email alerts as Unicode text	Seleccione esta opción para enviar mensajes de correo electrónico como texto Unicode en lugar del formato HTML o RTF.
Format Email Message	Opcionalmente, en el menú desplegable Format Email Message, seleccione el tipo de registro (Windows®, registros de texto, Syslog) y personalice el contenido del correo electrónico.

3. Haga clic en **Apply** y **OK**.

11.2.2 Alertas a través de la red

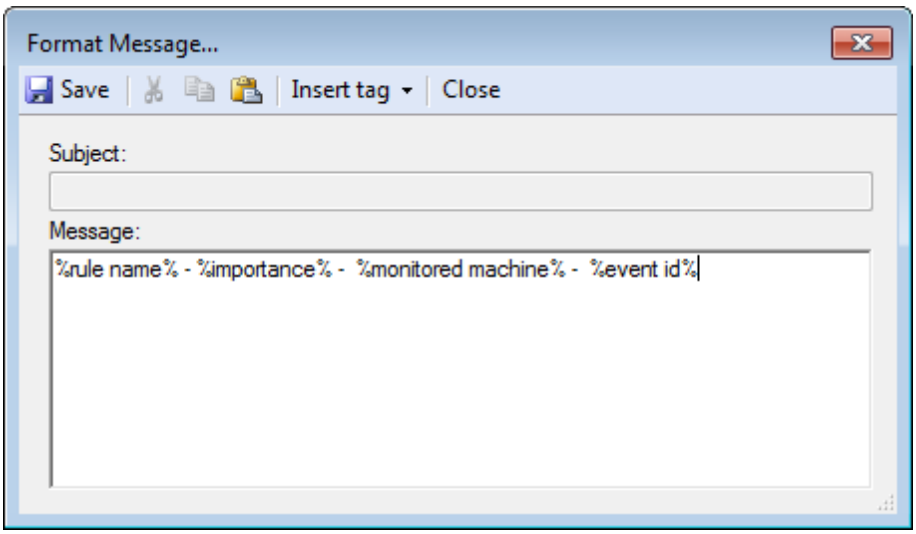

Alerting Options
Email
Network
SMS
SNMP
General
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending 'net send' alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Windows Events Alerts
Syslog Alerts
W3C Logs Alerts
SNMP Traps Alerts
SQL Server Audit Alerts
Oracle Server Audit Alerts
th computers and users. In
gged on so as to
successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Captura de pantalla 167: Configurar opciones de red

Para configurar alertas a través de la red:

1. En el cuadro de diálogo Alerting options, haga clic en la ficha **Network**.

2. En el menú desplegable **Format network message…**, seleccione el tipo de registro y personalice el formato del mensaje.

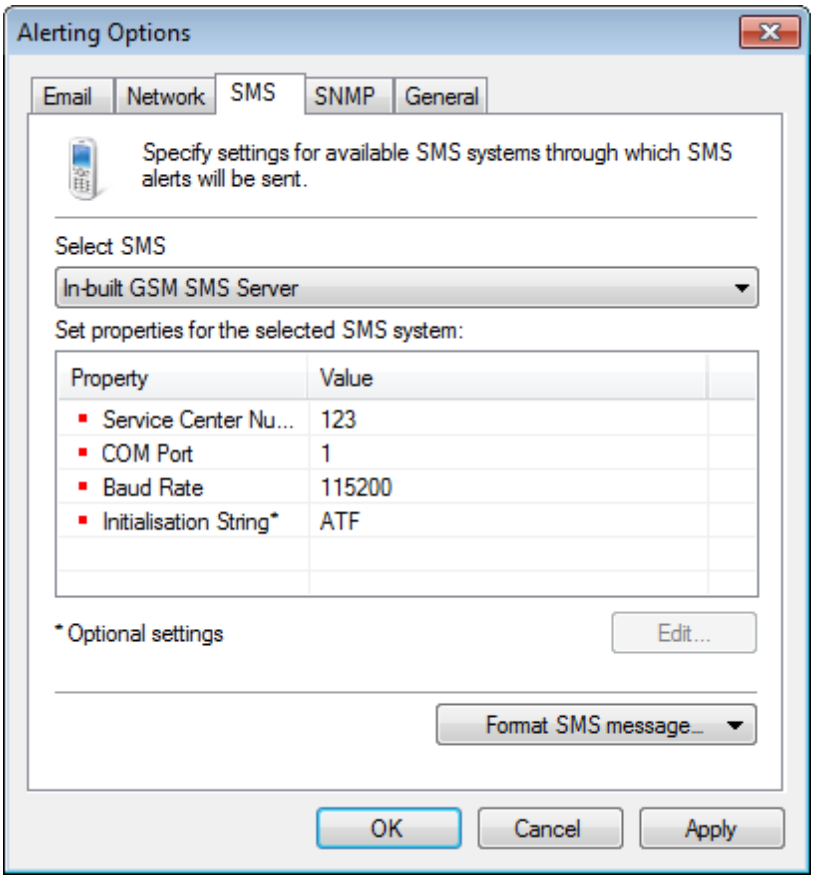


Captura de pantalla 168: Configurar alertas a través de la red: Dar formato a mensaje

3. Haga clic en **Insert tag** para seleccionar de una lista de etiquetas para incluir en el mensaje.

4. Haga clic en **Save** y en **OK**.

11.2.3 Alertas por SMS



Captura de pantalla 169: Configurar opciones de SMS

Para configurar alertas por SMS:

1. En el cuadro de diálogo Alerting options, haga clic en la ficha **SMS**.

2. Configure las opciones que se describen a continuación:

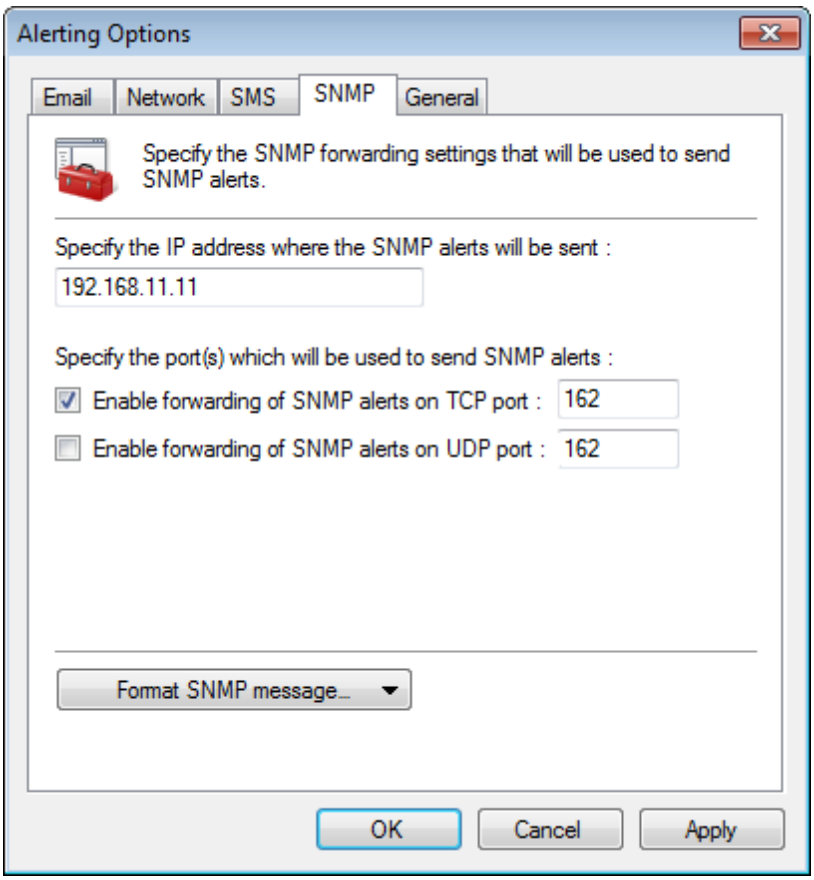
Tabla 76: Cuadro de diálogo Alerting Options: SMS

Opción	Descripción
Select SMS	Permite seleccionar el servicio de SMS que se utiliza para enviar alertas por SMS. Los servicios disponibles incluyen: » In-built GSM SMS Server » FaxMaker SMS service provider template » Clickatell Email2SMS Service » Generic SMS service provider template
Set properties for the selected SMS system	Permite configurar las propiedades para el tipo de servicio de SMS seleccionado. Entre otras, se incluyen las siguientes configuraciones de propiedades: » Service center number » COM Port » Baud Rate » Servidor SMTP » SMTP Port Haga clic en **Edit…** para configurar la propiedad seleccionada.
Format SMS message	Opcionalmente, en el menú desplegable **Format Email Message**, seleccione el tipo de registro (Windows®, registros de texto, Syslog) y personalice el contenido del correo electrónico.

3. Haga clic en **Apply** y **OK**.

11.2.4 Alertas a través de SNMP

Para configurar alertas a través de capturas SNMP:



Captura de pantalla 170: Configurar alertas a través de capturas SNMP

1. En el cuadro de diálogo **Alerting Options**, haga clic en la ficha **SNMP**.

2. Configure las opciones que se describen a continuación:

Tabla 77: Opciones de alerta: Capturas SNMP

Opción	Descripción
Specify the IP address where the SNMP alerts will be sent	Ingrese la dirección IP del destinatario.
Specify the port(s) which will be used to send SNMP alerts	Especifique el puerto de comunicación TCP/UDP. De forma predeterminada, el puerto asignado es el 162.
Format SNMP message	Opcionalmente, en el menú desplegable Format Email Message, seleccione el tipo de registro (Windows®, registros de texto, Syslog) y personalice el contenido del correo electrónico.

3. Haga clic en **Apply** y **OK**.

11.2.5 Configuración general

Para configurar opciones de alerta generales:

1. En el cuadro de diálogo **Alerting Options**, haga clic en la ficha **General**.

2. Configure las opciones que se describen a continuación y haga clic en **OK**:

Tabla 78: Opciones de alerta: Configuración general

Opción	Descripción
Send email alerts on database errors	Las alertas de correo electrónico se envían cuando ocurren errores en una base de datos, como error de copia de seguridad, daños de datos, el tamaño excede el tamaño máximo especificado y otros errores de operación de alguna base de datos.

12 Grupos de usuarios

En este capítulo, se proporciona información relacionada con la creación y administración de usuarios y grupos. A través de los nodos Users y Groups, se pueden crear usuarios y grupos y se pueden asignar alertas, horarios de trabajo y otras propiedades específicas a cada usuario y grupo, mientras que se pueden asignar diferentes derechos de acceso a la consola para cada usuario de los nodos Console Security y Audit Options.

Temas de este capítulo:

12.1 Configurar la cuenta del administrador 225

12.2 Administrar cuentas de usuario 232

12.3 Administrar grupos de usuarios 239

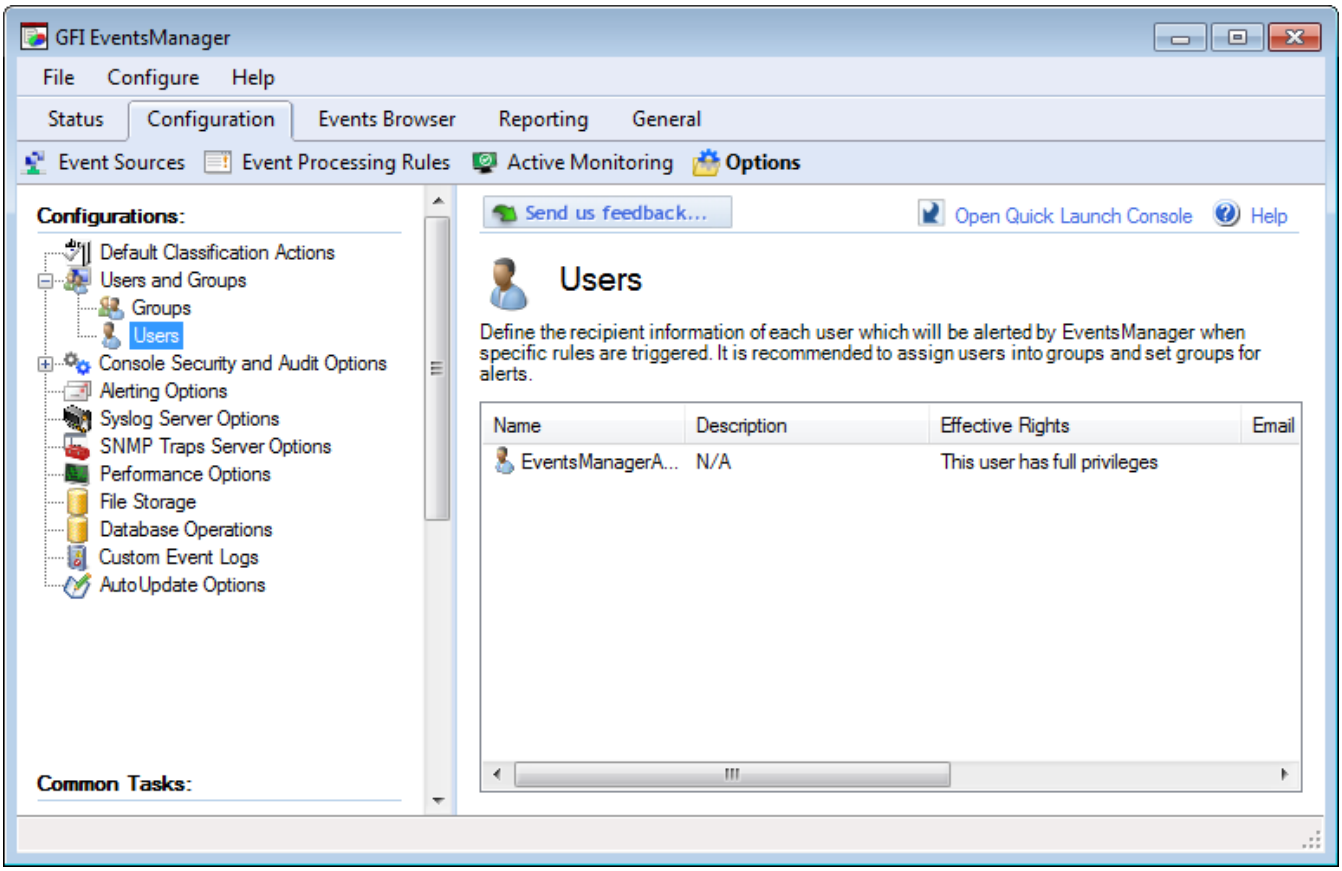
12.1 Configurar la cuenta del administrador

GFI EventsManager crea automáticamente una cuenta **EventsManagerAdministrator**. Sin embargo, todavía debe configurar algunas propiedades, como las direcciones de notificación y la seguridad de la cuenta.

> **Nota**
>
> GFI EventsManager requiere una dirección de correo electrónico de administrador válida para distribuir alertas automáticas cuando se detectan eventos particulares.

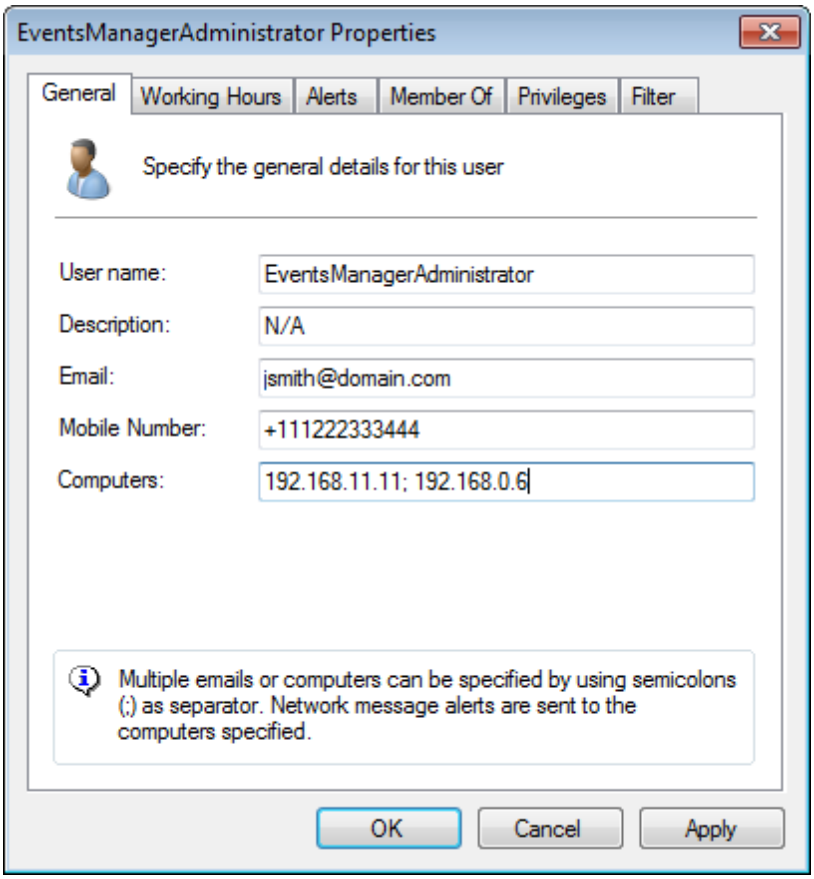
Para configurar la cuenta de administrador de GFI EventsManager:

1. En la ficha **Configuration> Options**, expanda **Users and Groups > Users**.



Captura de pantalla 171: Configurar cuenta EventsManagerAdministrator

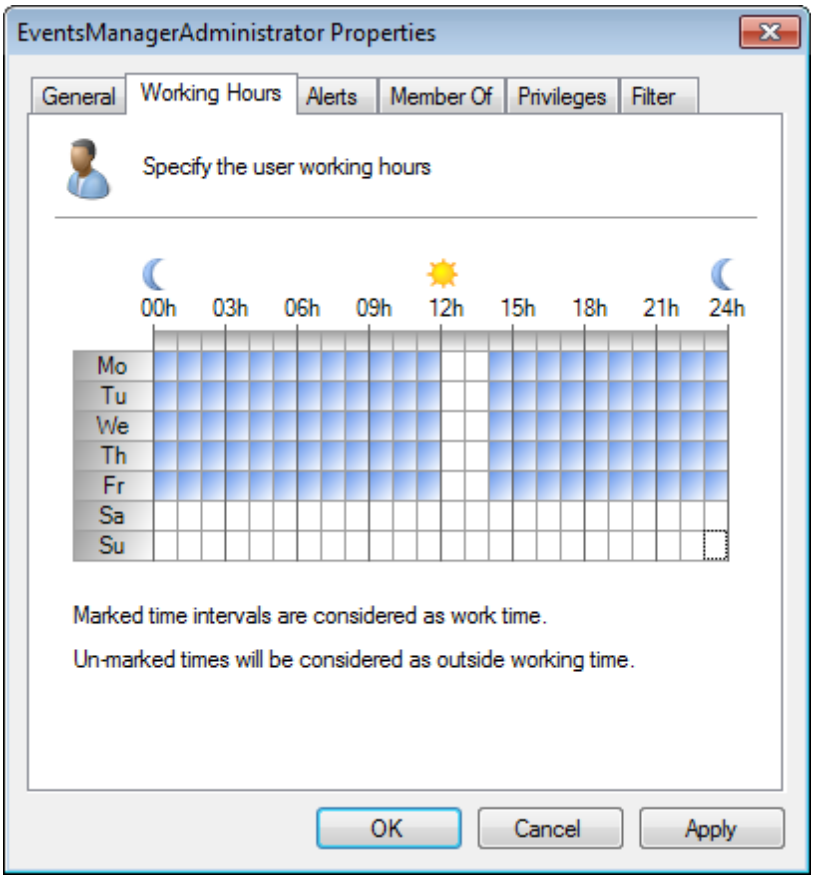
2. En el panel derecho, haga clic con el botón secundario en **EventsManagerAdministrator** y haga clic en **Properties**.



Captura de pantalla 172: Propiedades de EventsManagerAdministrator

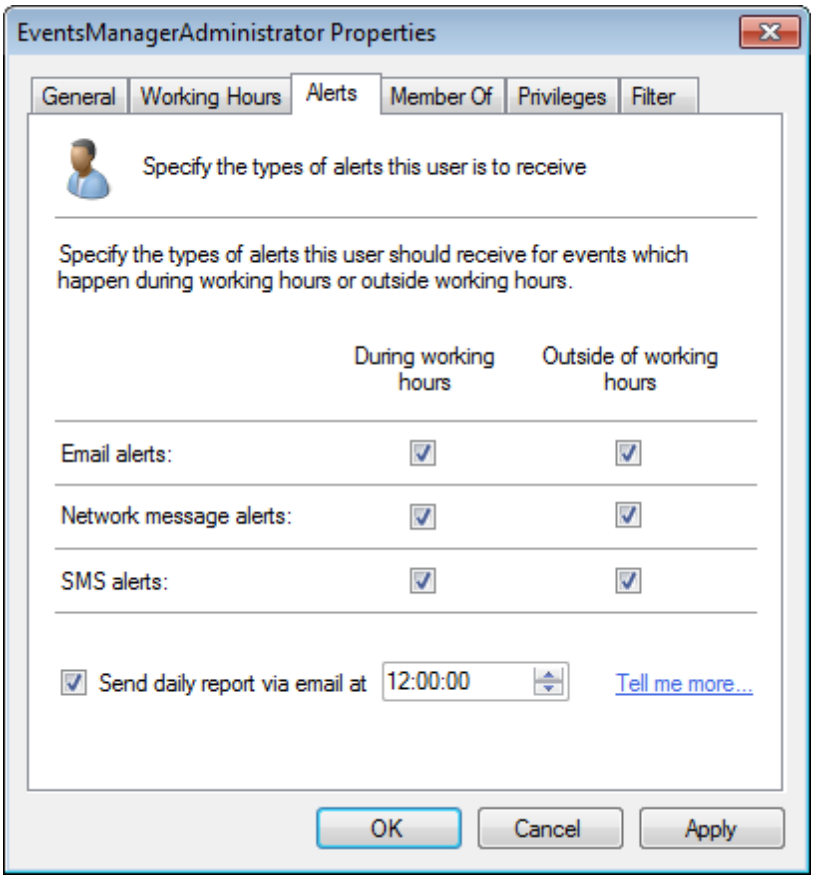
3. En la ficha **General**, especifique:

- Un nombre de usuario para la cuenta de administrador de GFI EventsManager
- (Opcional) Una descripción de la cuenta
- Una dirección de correo electrónico válida para distribución de alertas por correo electrónico
- Un número de celular válido para la distribución de alertas por SMS
- Una IP o nombre de equipo válido para la distribución de alertas a través de la red



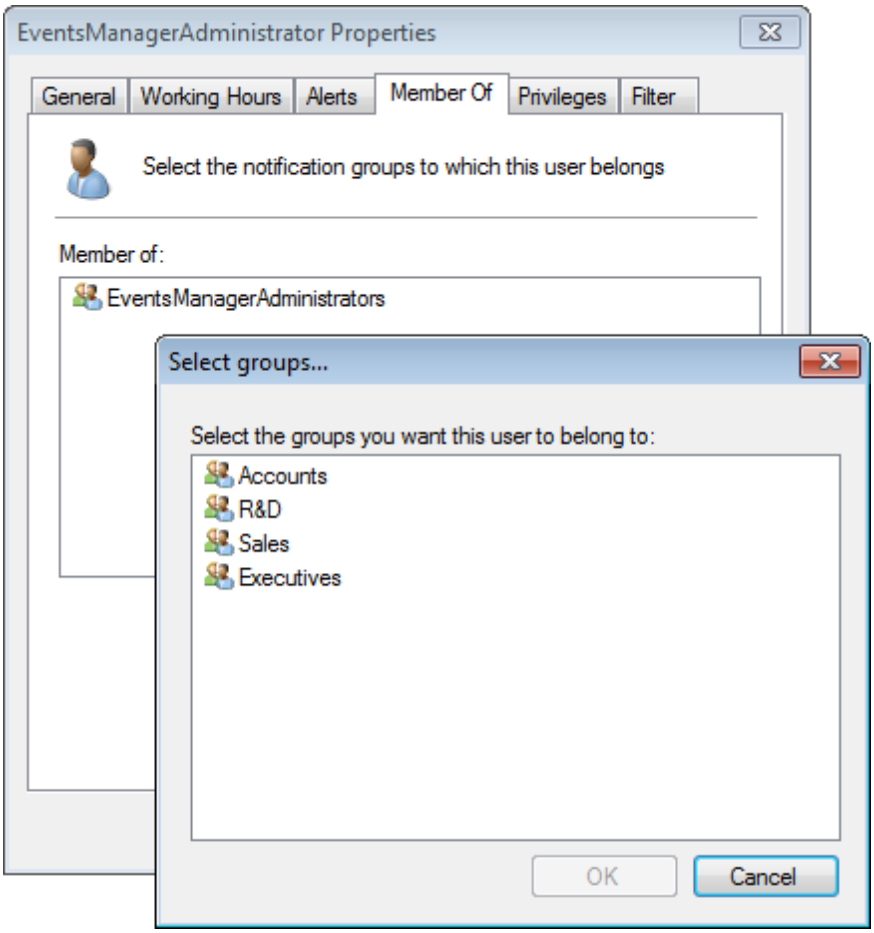
Captura de pantalla 173: Configurar horas de trabajo habituales del usuario

4. Haga clic en la ficha **Working Hours** y especifique las horas de trabajo habituales del administrador. Los intervalos de tiempo marcados se consideran horas de trabajo.



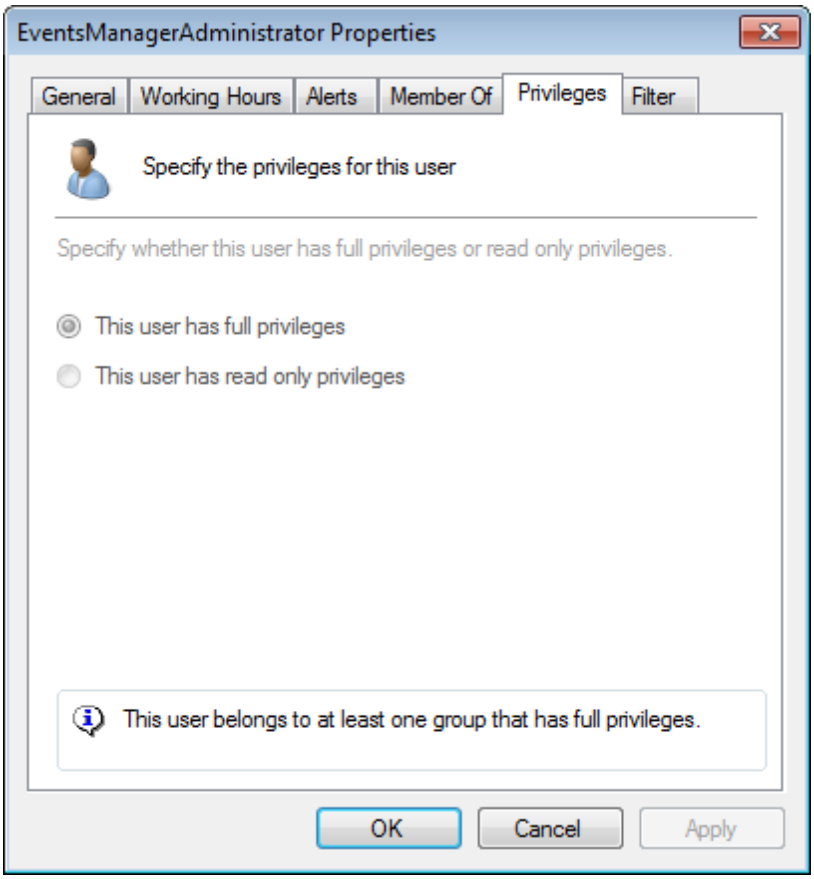
Captura de pantalla 174: Configurar alertas fuera del horario de trabajo

5. Haga clic en la ficha **Alerts** y seleccione las alertas enviadas durante las horas de trabajo y fuera de las horas de trabajo. Opcionalmente, seleccione **Send daily report via email at** y especifique la hora para enviar un correo electrónico que incluya la actividad diaria.



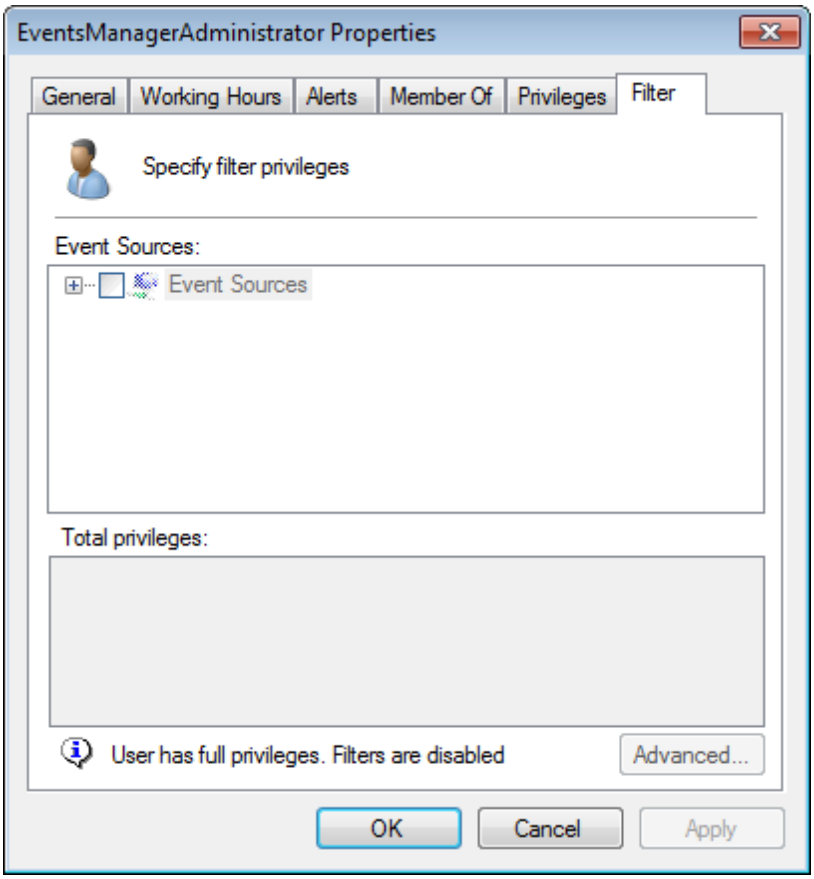
Captura de pantalla 175: Seleccione el grupo del cual es miembro la cuenta de usuario

6. Haga clic en la ficha **Member Of** y seleccione los grupos de notificación a los que pertenece el usuario. De forma predeterminada, el administrador es un miembro del grupo de notificación **EventsManagerAdministrators**.



Captura de pantalla 176: Configurar privilegios de la cuenta de usuario

7. Haga clic en la ficha **Privileges** para editar los privilegios del usuario. De forma predeterminada, la cuenta EventsManagerAdministrator tiene privilegios plenos y no se puede modificar.



Captura de pantalla 177: Filtrar cuenta de usuario

8. Haga clic en la ficha **Filter** para editar lo que el administrador puede ver en la consola de administración. De forma predeterminada, esta ficha está inhabilitada para la cuenta EventManagerAdministartor.

9. Haga clic en **Apply** y **OK**.

12.2 Administrar cuentas de usuario

GFI EventsManager le permite crear una lista personalizada de los usuarios que se pueden organizar en grupos para agilizar las tareas administrativas.

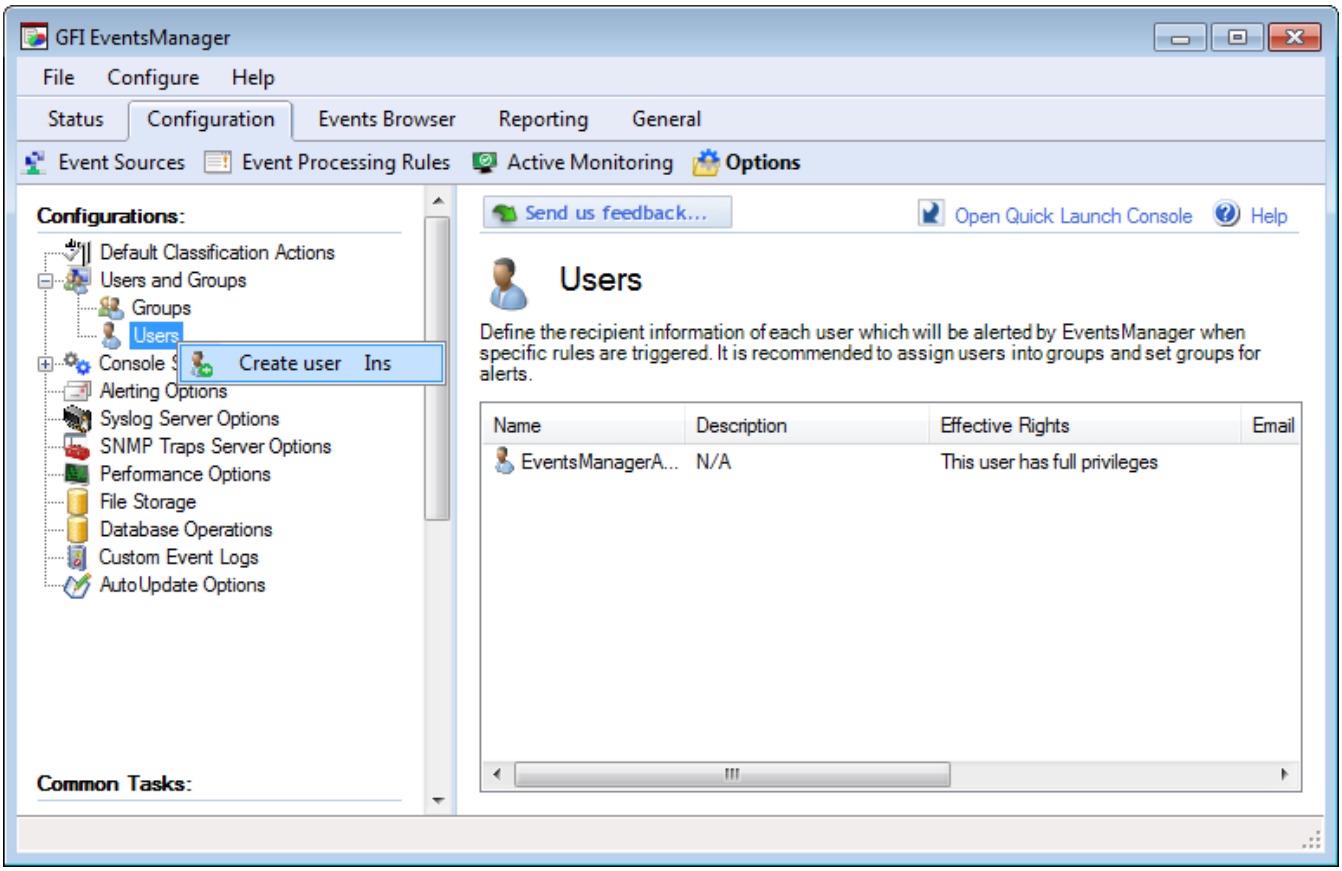
Esta sección contiene información acerca de:

- Crear una nueva cuenta de usuario
- Cambiar las propiedades de la cuenta de usuario
- Eliminar una cuenta de usuario

12.2.1 Crear una nueva cuenta de usuario

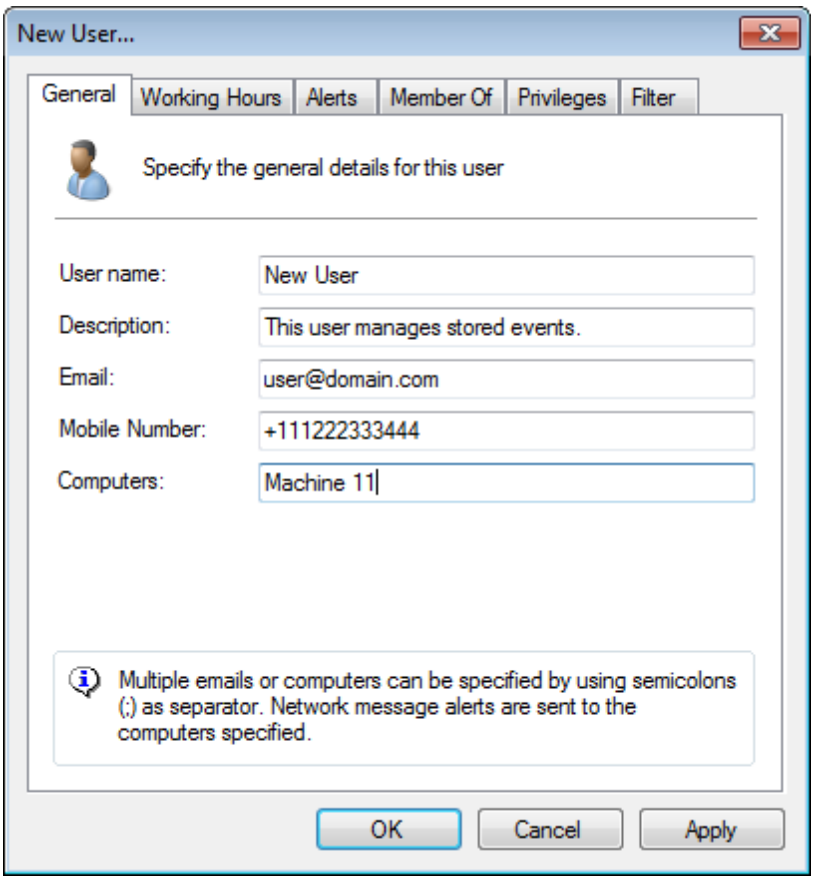
Para crear un nuevo usuario:

1. En la ficha **Configuration > Options**, amplíe el nodo **Users and Groups**.



Captura de pantalla 178: Crear un nuevo usuario

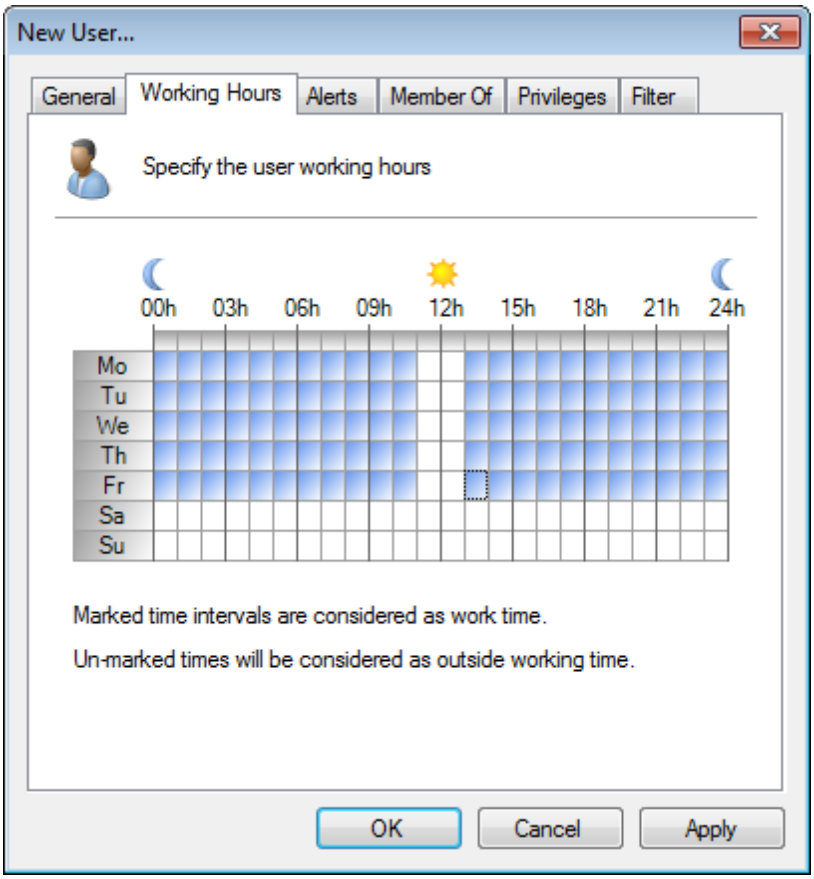
2. Haga clic con el botón secundario en el subnodo **Users** y seleccione **Create user…**.



Captura de pantalla 179: Crear un nuevo usuario - Propiedades generales

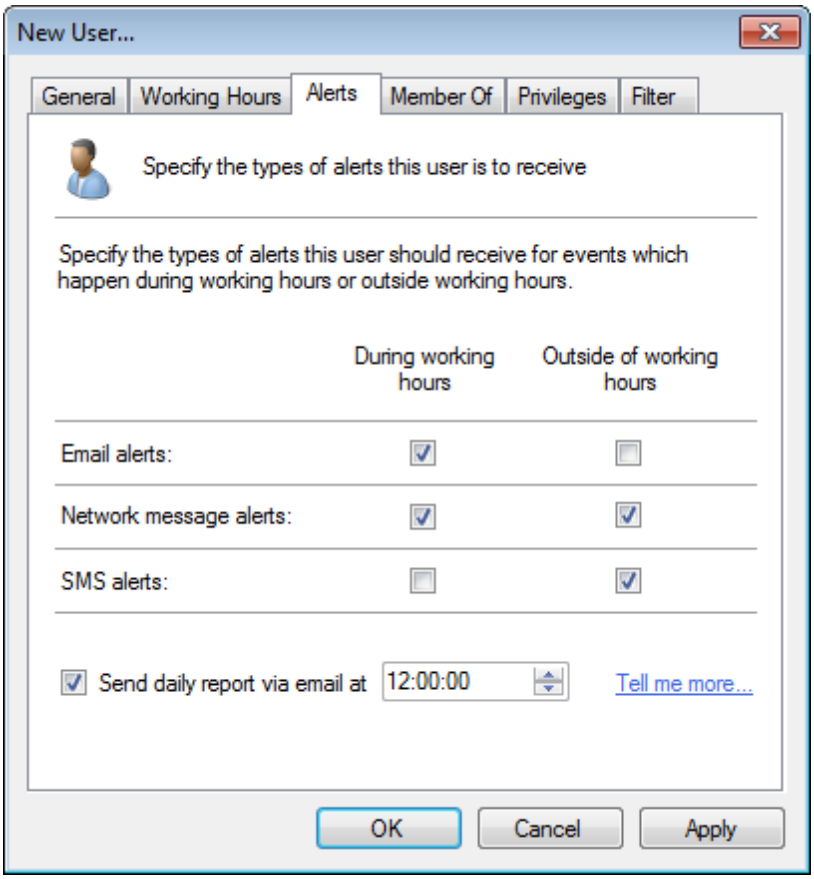
3. En la ficha **General**, especifique:

- Un nombre de usuario para la cuenta de usuario
- (Opcional) Una descripción de la cuenta
- Una dirección de correo electrónico válida para distribución de alertas por correo electrónico
- Un número de celular válido para la distribución de alertas por SMS
- Una IP o nombre de equipo válido para la distribución de alertas a través de la red



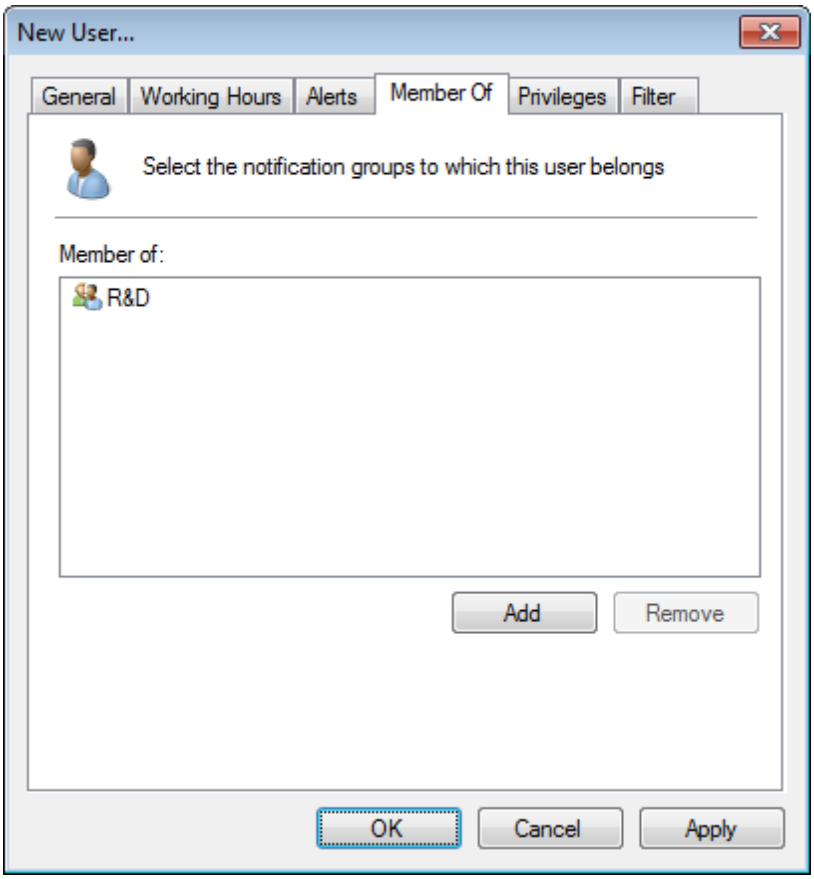
Captura de pantalla 180: Crear un nuevo usuario - Horas de trabajo

4. Haga clic en la ficha **Working Hours** y especifique las horas de trabajo habituales del nuevo usuario. Los intervalos de tiempo marcados se consideran horas de trabajo.



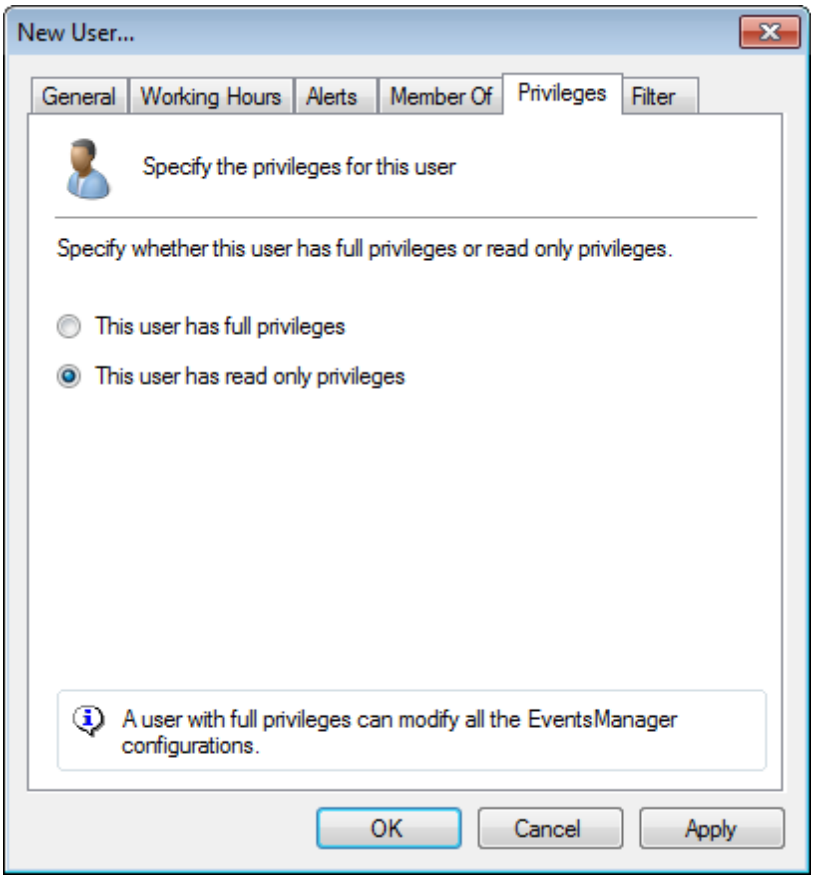
Captura de pantalla 181: Crear un nuevo usuario - Opciones de alerta

5. Haga clic en la ficha **Alerts** y seleccione las alertas enviadas durante las horas de trabajo y fuera de las horas de trabajo. Opcionalmente, seleccione **Send daily report via email at** y especifique la hora para enviar un correo electrónico que incluya la actividad diaria. Para obtener más información, consulte Alertas y acciones predeterminadas (página 216).



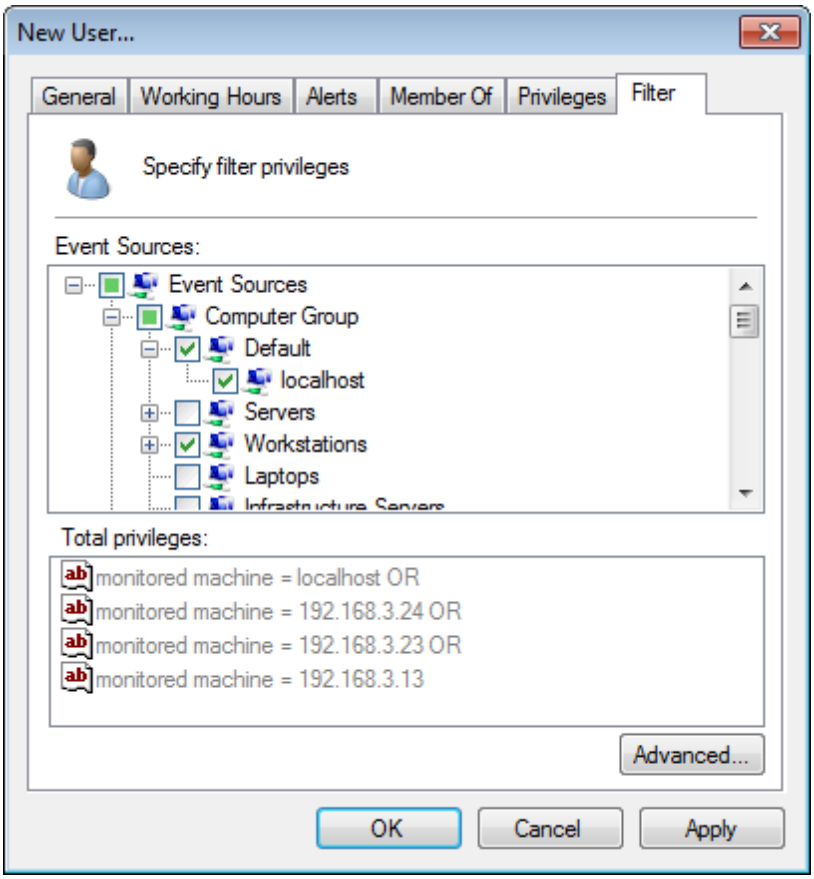
Captura de pantalla 182: Crear un nuevo usuario - Seleccionar grupos de notificación

6. Haga clic en la ficha **Member Of** y haga clic en **Add**. Seleccione los grupos de notificación a los que pertenece el usuario y haga clic en **OK**.



Captura de pantalla 183: Crear un nuevo usuario - Privilegios

7. Haga clic en la ficha **Privileges** para configurar los privilegios del usuario. De forma predeterminada, las nuevas cuentas de usuario solamente tienen privilegios de lectura.



Captura de pantalla 184: Opciones de filtrado de usuarios

8. Haga clic en la ficha **Filter** para configurar lo que se le permite mostrar al nuevo usuario en la consola de administración. En la siguiente tabla, se describen las opciones disponibles:

Tabla 79: Opciones de filtrado de usuarios

Opción	Descripción
Event Sources	GFI EventsManager le proporciona un conjunto de condiciones preconfiguradas para filtrar orígenes de eventos. Seleccione los orígenes de eventos que desea que sean visibles para el usuario.
Total privileges	Haga clic en **Advanced...** para iniciar el cuadro de diálogo **Advanced Filtering**. Este cuadro de diálogo le permite compilar sus propias condiciones para el filtrado granular, lo cual le permite filtrar los eventos que contienen atributos específicos. Para agregar una condición: 1. En el cuadro de diálogo **Advanced Filtering**, haga clic en **Add** y seleccione un campo de la lista. Ejemplo: Date, Importance, Log format. 2. En el campo seleccionado, seleccione un operador del menú desplegable **Field operator**. Ejemplo: Equal to, Less than, Greater than. 3. Especifique un valor para el operador en el cuadro de texto **Field value**. 4. Haga clic en **Aceptar**. 5. Repita los Pasos 1 a 4 para agregar más de un nombre de campo. **Nota** Para obtener más información, consulte Definir restricciones de consulta.

9. Haga clic en **Apply** y **OK**.

12.2.2 Cambiar propiedades de la cuenta de usuario

Para editar propiedades de usuario:

1. En la ficha **Configuration > Options**, amplíe el nodo **Users and Groups**.

2. En el subnodo **Users**, haga clic con el botón secundario en un usuario y seleccione **Properties**.

3. Haga los cambios necesarios en las fichas disponibles y haga clic en **OK**.

12.2.3 Eliminar una cuenta de usuario

Para eliminar un usuario:

1. En la ficha **Configuration> Options**, expanda el nodo **Users and Groups** y seleccione **Users**.

2. En el panel derecho, haga clic con el botón secundario en un usuario y seleccione **Delete**.

12.3 Administrar grupos de usuarios

GFI EventsManager le permite asignar usuarios a un grupo. Una vez que se hayan configurado las propiedades del grupo, cada miembro del grupo hereda la misma configuración.

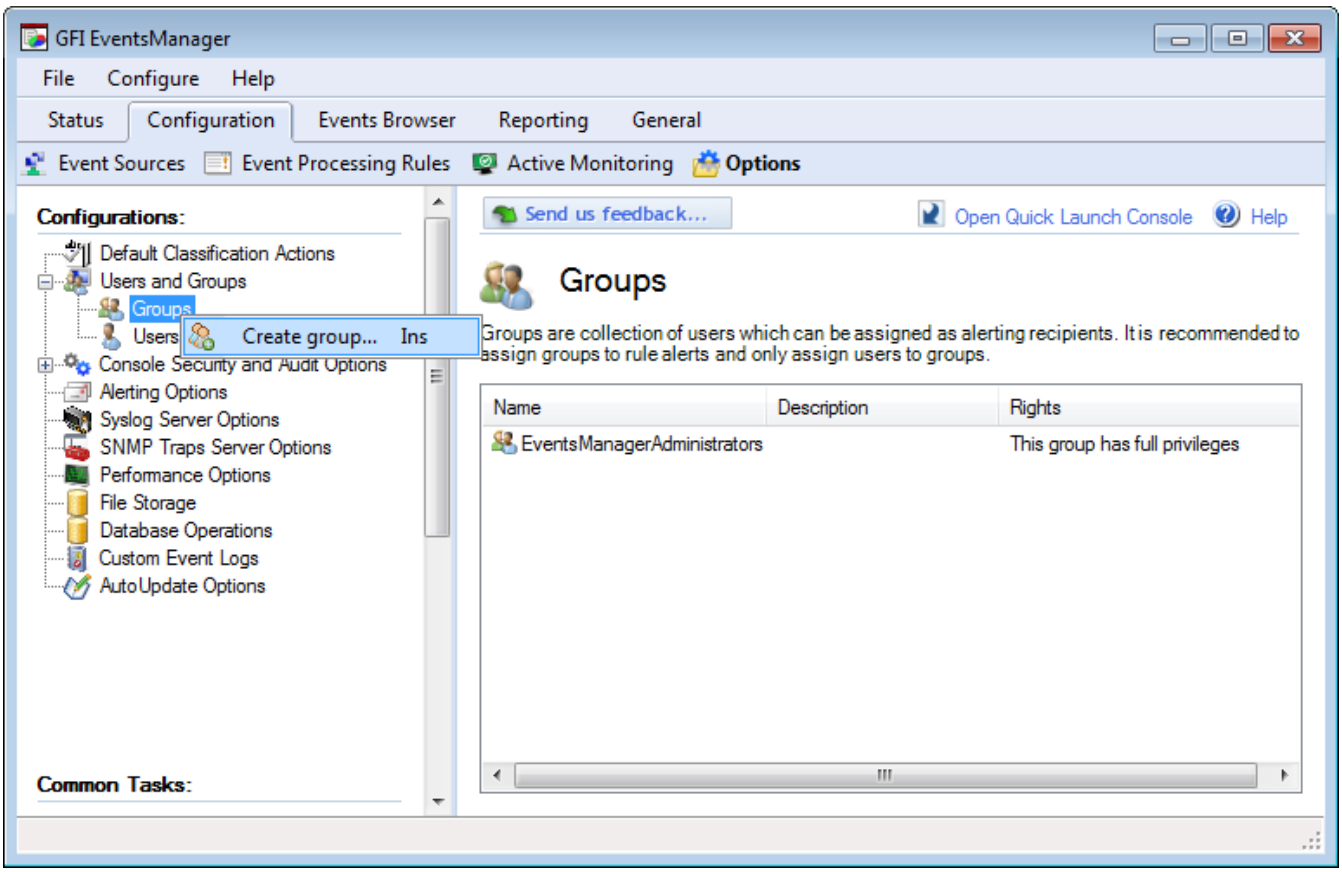
Esta sección contiene información acerca de:

- Crear un nuevo grupo
- Cambiar propiedades de un grupo
- Eliminar un grupo

12.3.1 Crear un nuevo grupo

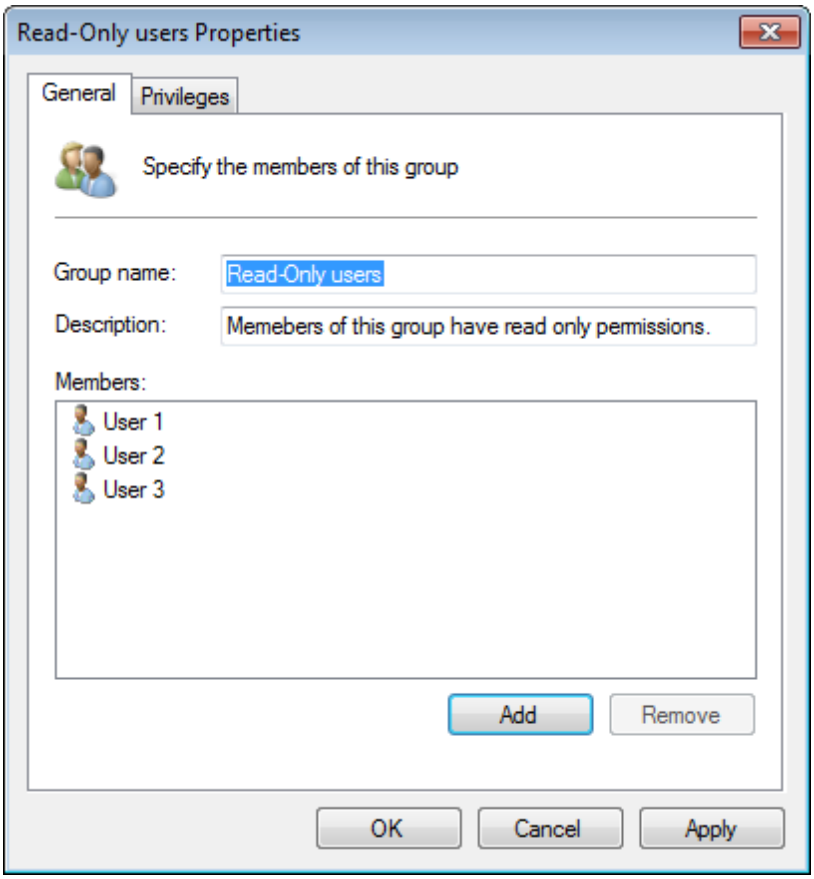
Para crear un nuevo grupo de usuarios:

1. En la ficha **Configuration** > **Options**, amplíe el nodo **Users and Groups**.



Captura de pantalla 185: Crear un nuevo grupo de usuarios

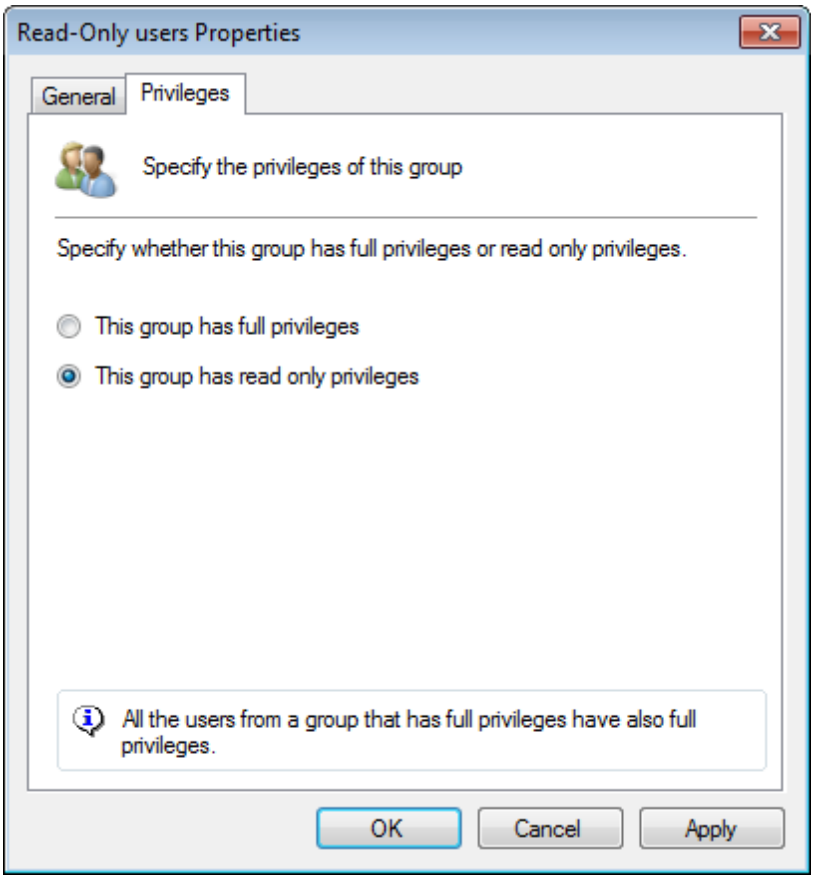
2. Haga clic con el botón secundario en el subnodo **Groups** y seleccione **Create group…**.



Captura de pantalla 186: Crear un nuevo grupo de usuarios - Propiedades generales

3. Especifique el nombre y una descripción opcional para el nuevo grupo.

4. Haga clic en **Add** para agregar usuarios al grupo.


Read-Only users Properties
General
Privileges
Specify the privileges of this group
Specify whether this group has full privileges or read only privileges.
This group has full privileges
This group has read only privileges
All the users from a group that has full privileges have also full privileges.
OK
Cancel
Apply

Captura de pantalla 187: Crear un nuevo grupo de usuarios - Propiedades generales

5. En la ficha **Privileges**, determine si el grupo tiene permisos **Full** o **Read Only**; es decir, plenos o de solo lectura.

6. Haga clic en **Apply** y **OK**.

12.3.2 Cambiar propiedades de un grupo

Para editar la configuración de un grupo de usuarios:

1. En la ficha **Configuration** > **Options**, amplíe el nodo **Users and Groups**.

2. En el panel derecho, haga clic con el botón secundario en el grupo que desea configurar y seleccione **Properties**.

3. Realice los cambios necesarios en las fichas disponibles y haga clic en **OK**.

12.3.3 Eliminar un grupo

Para eliminar un grupo de usuarios:

1. En la ficha **Configuration** > **Options**, amplíe el nodo **Users and Groups**.

2. Haga clic con el botón secundario en el grupo que desea eliminar y seleccione **Delete**.

13 Opciones de auditoría y seguridad de la consola

Las opciones de seguridad de la consola y auditoría le permiten proteger GFI EventsManager contra los accesos no autorizados y los intentos malintencionados. Las opciones de auditoría proporcionadas le permiten supervisar con precisión la actividad de GFI EventsManager.

Temas de este capítulo:

13.1 Activar sistema de inicio de sesión 242

13.2 Ocultación de identidad 245

13.3 Auditar actividad de la consola 248

13.4 Credenciales de detección automática 249

13.1 Activar sistema de inicio de sesión

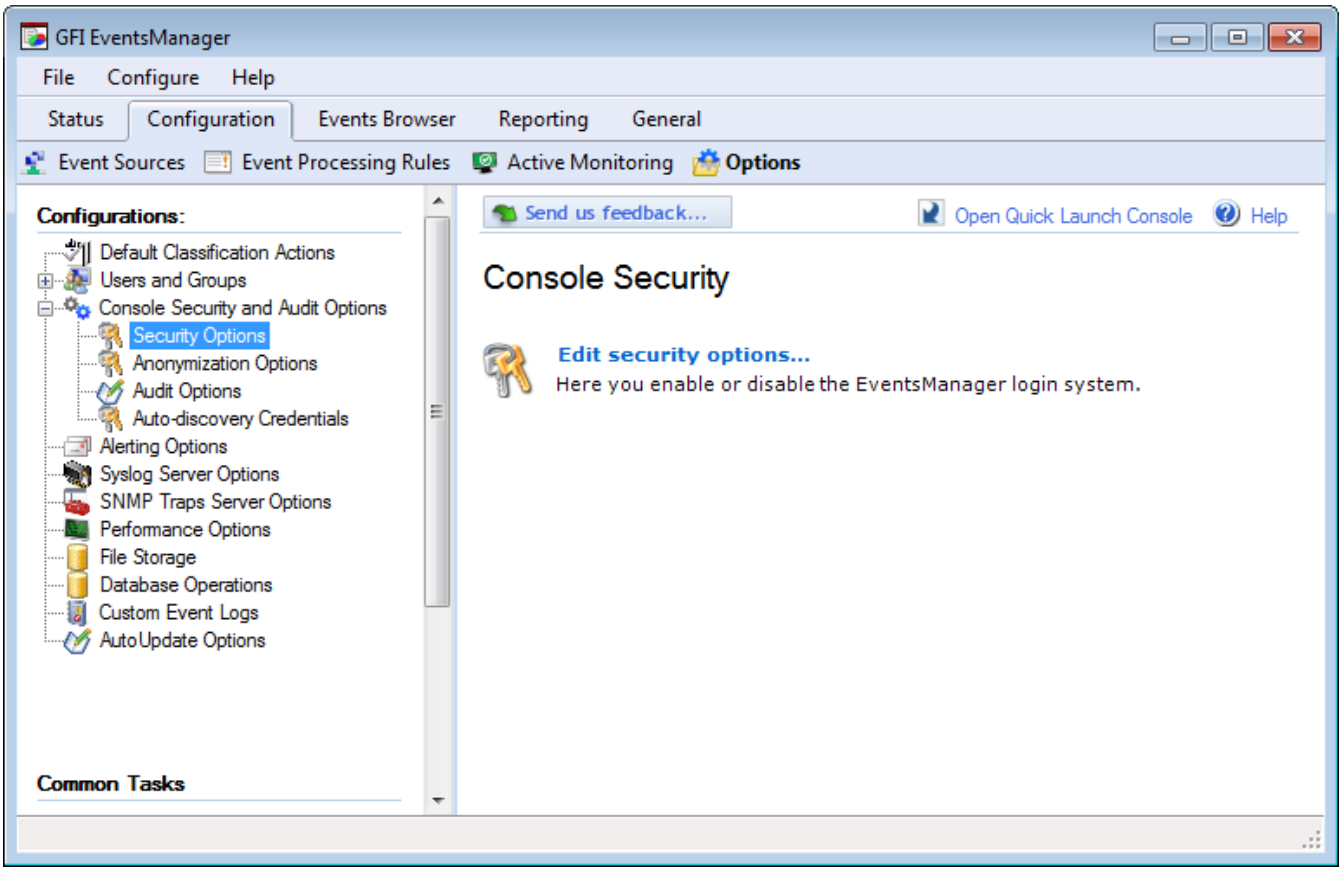
Cuando el sistema de inicio de sesión está habilitado se les solicitará a todos los usuarios que especifiquen sus credenciales cada vez que inicien la consola de administración de GFI EventsManager.

Nota

Antes de activar el sistema de inicio de sesión, debe configurar los parámetros del servidor de correo electrónico. Para obtener más información, consulte Configurar opciones de alerta.

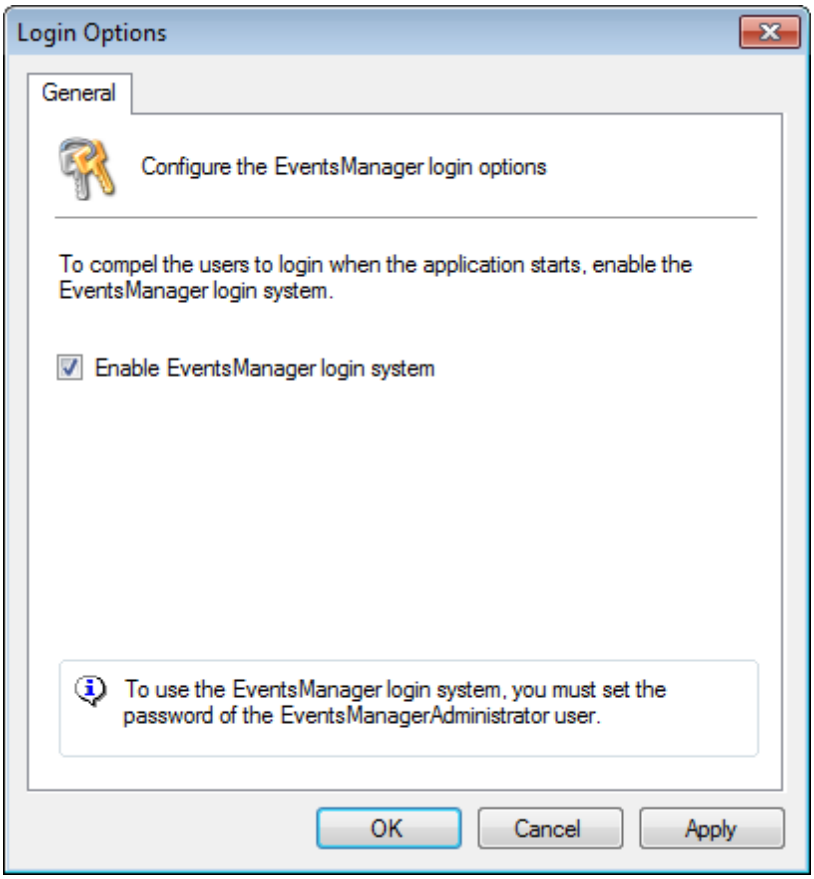
Para habilitar el sistema de inicio de sesión:

1. En la ficha **Configuration> Options**, expanda el nodo **Console Security and Audit Options**.



Captura de pantalla 188: Editar opciones de seguridad de la consola

2. Expanda el nodo **Console Security and Audit Options**, haga clic con el botón secundario en el nodo **Security Options** y seleccione **Edit security options…**.


Login Options
General
Configure the EventsManager login options
To compel the users to login when the application starts, enable the EventsManager login system.
Enable EventsManager login system
To use the EventsManager login system, you must set the password of the EventsManagerAdministrator user.
OK
Cancel
Apply

Captura de pantalla 189: Habilitar sistema de inicio de sesión de EventsManager

3. Seleccione **Enable EventsManager login system** para permitir el inicio de sesión.

4. Haga clic en **Apply** y **OK**.

Nota

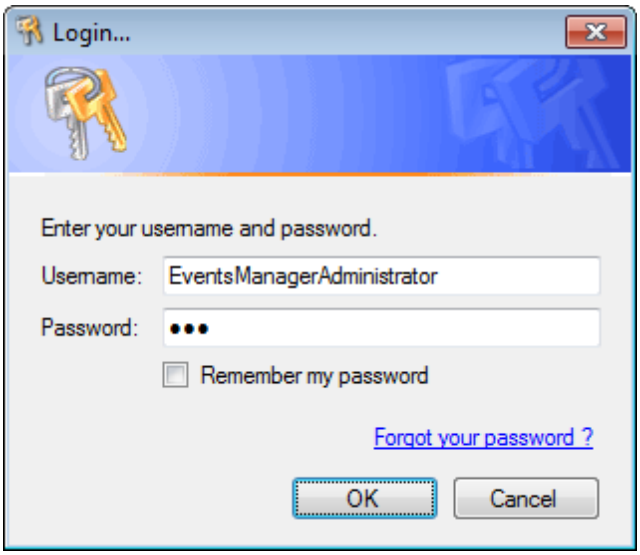
Para configurar o modificar las contraseñas de usuario, vaya a la ficha **Configuration> Users and Groups > Users**, haga clic con el botón secundario en la cuenta de usuario y seleccione **Change Password**.

Importante

Una vez que el sistema de inicio de sesión está habilitado, los usuarios deben iniciar sesión en la consola especificando su nombre de usuario y contraseña, y deben tener configurada una dirección de correo electrónico válida para poder recuperar contraseñas perdidas. Para obtener más información, consulte Administrar cuentas de usuario.

13.1.1 Recuperación de contraseña

Cuando está activado el sistema de inicio de sesión de GFI EventsManager, se les solicita a todos los usuarios que ingresen una contraseña y un nombre de usuario válidos para acceder a la consola de administración.



Captura de pantalla 190: Solicitud de credenciales de inicio de sesión

Si olvida o pierde una contraseña:

1. Ingrese su nombre de usuario.

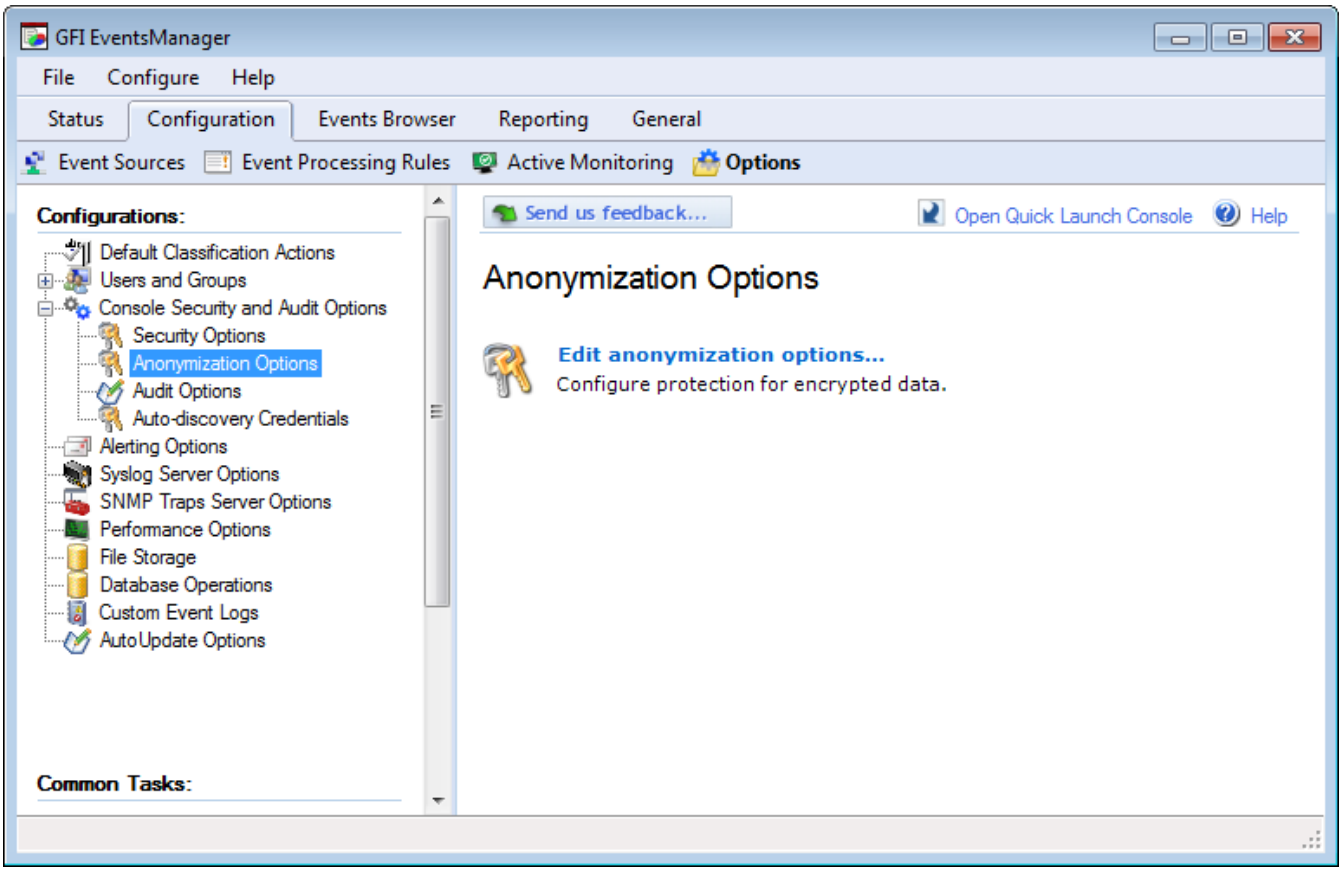
2. Haga clic en el vínculo **Forgot your password?**. GFI EventsManager le enviará un correo electrónico con su contraseña de inicio de sesión a la dirección de correo electrónico especificada durante la configuración de la cuenta de usuario.

13.2 Ocultación de identidad

En algunos países, las leyes de privacidad establecen que está en contra de la ley no cifrar la información personal recuperada por las aplicaciones de supervisión para la protección de la privacidad. GFI EventsManager le permite cifrar información personal al exportar o ver los registros de eventos.

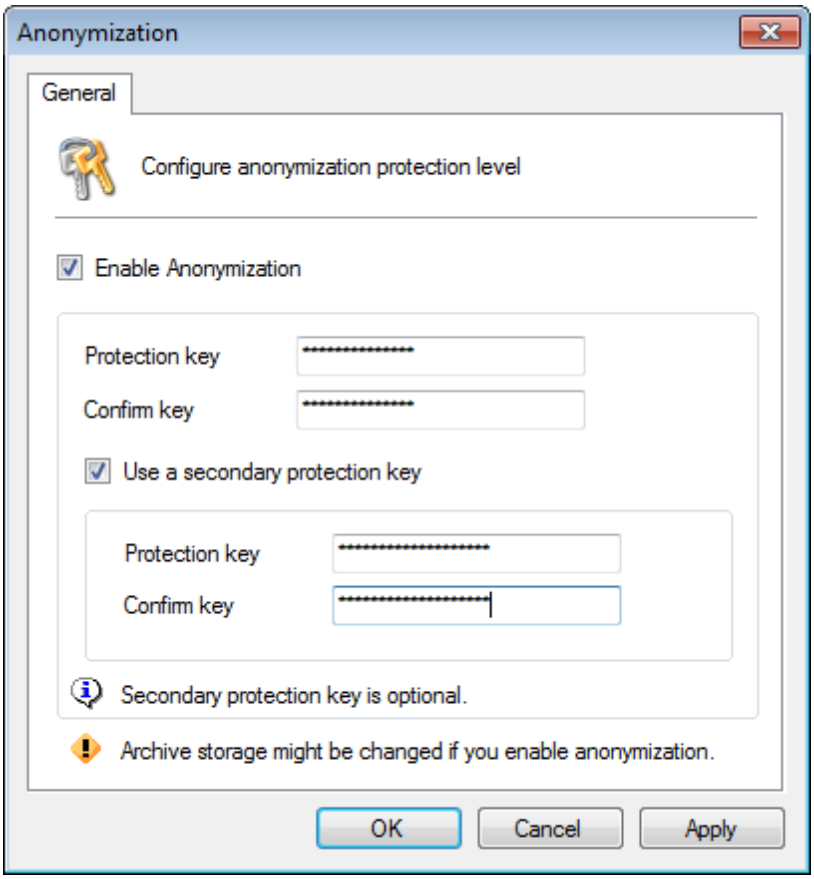
Active la anonimización para cifrar toda la información personal. El Explorador de eventos y el panel pueden reconocer dicha información y no mostrarla. En su lugar, muestran mensajes **<cifrado>** o **anonimizados**.

Para configurar la anonimización:



Captura de pantalla 191: Activar la consola de anonimización

1. En la ficha **Configuration> Options**, expanda el nodo **Console Security and Audit Options**, haga clic con el botón secundario en **Anonymization** y haga clic en **Edit anonymization options…**.



Captura de pantalla 192: Opciones de anonimización

2. Seleccione **Enable Anonymization** e ingrese la contraseña de cifrado.

3. (Opcional) Seleccione **Use a secondary protection key** para utilizar dos contraseñas para cifrar el registro de eventos. Los registros de eventos solamente se pueden descifrar proporcionando dos claves de descifrado.

4. Haga clic en **Apply** y **OK**.

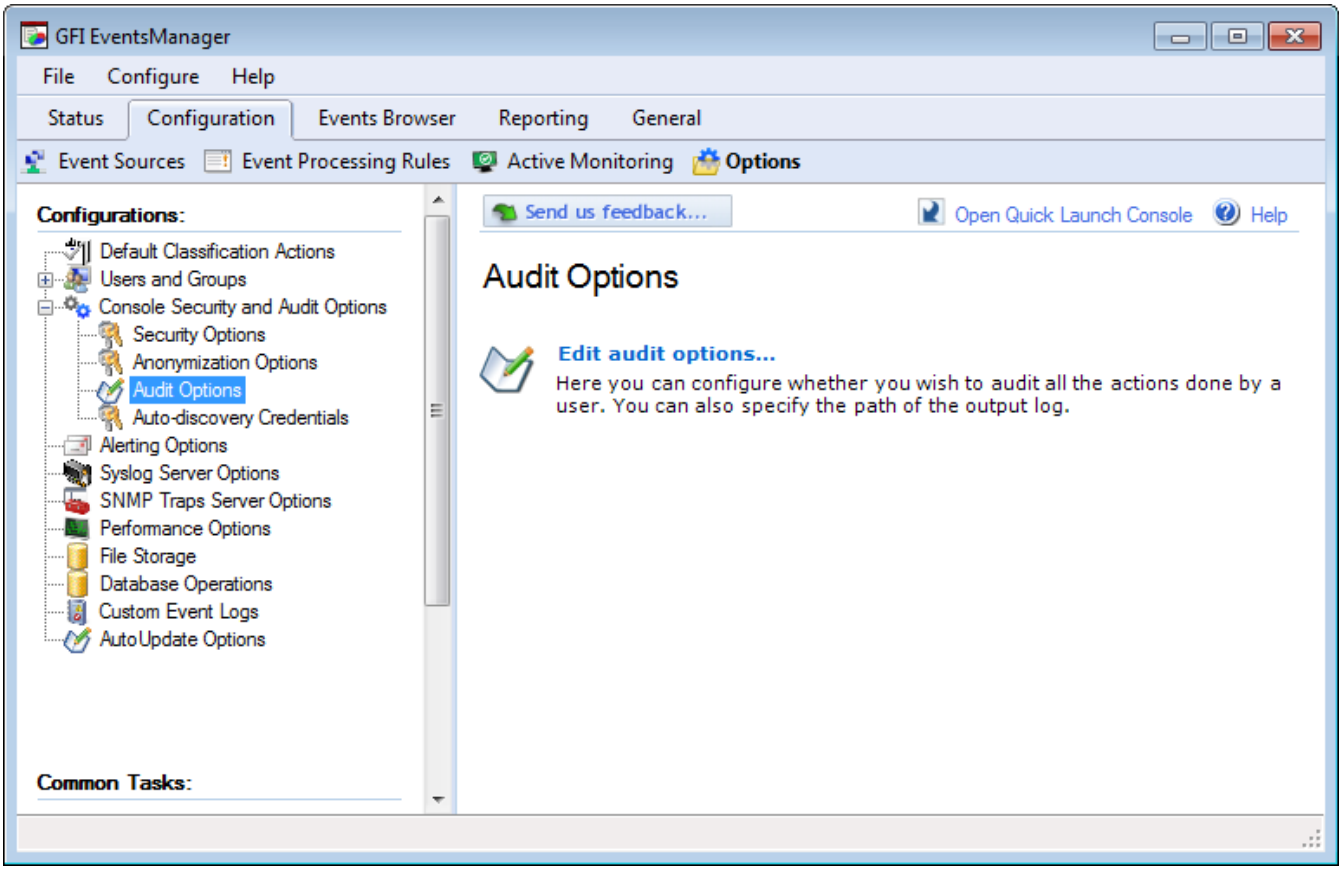
Nota

Una vez que está activada la anonimización, los datos personales se ocultan en:

- Cualquiera de las vistas de estado (General, Job Activity y Statistics)
- Explorador de eventos
- Informes
- Registros de eventos exportados/archivados (usted puede quitar la anonimización al importar los registros exportados)

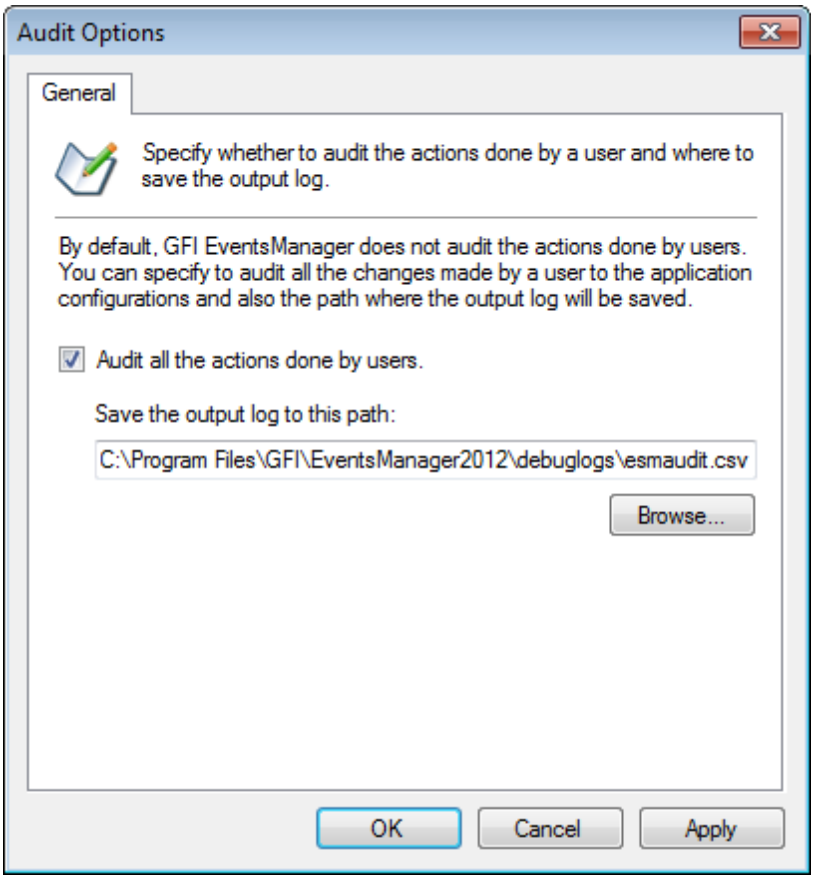
13.3 Auditar actividad de la consola

GFI EventsManager puede guardar la actividad de la consola en registros externos. Para configurar la auditoría de actividad de la consola:



Captura de pantalla 193: Activar auditoría de actividad del usuario de la consola

1. En la ficha **Configuration > Options**, amplíe el nodo **Console Security and Audit Options**.
2. Haga clic en **Audit Options** y seleccione **Edit audit options…**.


Audit Options
General
Specify whether to audit the actions done by a user and where to save the output log.
By default, GFI EventsManager does not audit the actions done by users. You can specify to audit all the changes made by a user to the application configurations and also the path where the output log will be saved.
Audit all the actions done by users.
Save the output log to this path:
C:\Program Files\GFI\EventsManager2012\debuglogs\esmaudit.csv
Browse...
OK
Cancel
Apply

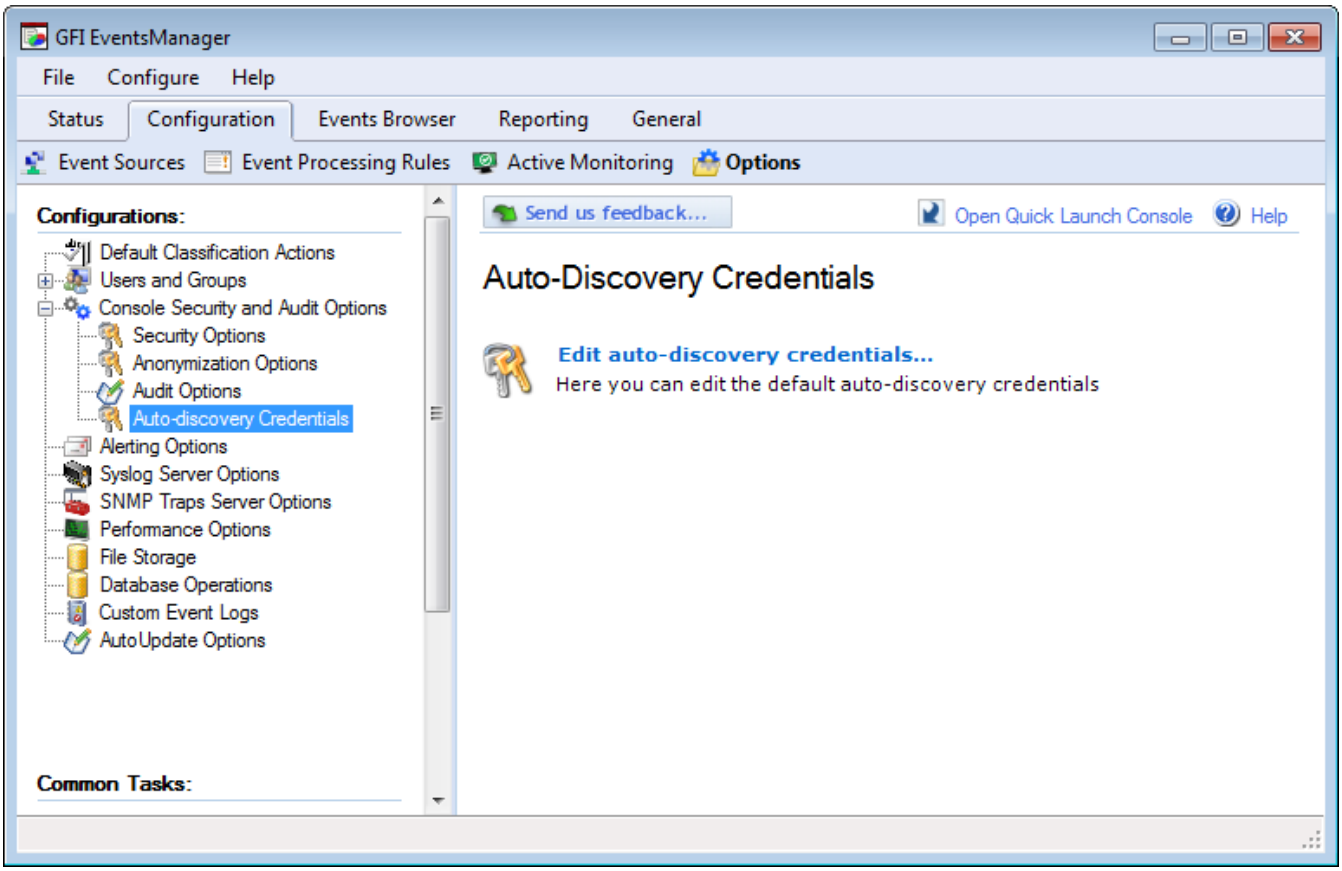
Captura de pantalla 194: Cuadro de diálogo Audit Options

3. Seleccione la opción **Audit all the actions done by users** y especifique la ubicación donde se guardará el archivo de registro de salida.

4. Haga clic en **Apply** y **OK**.

13.4 Credenciales de detección automática

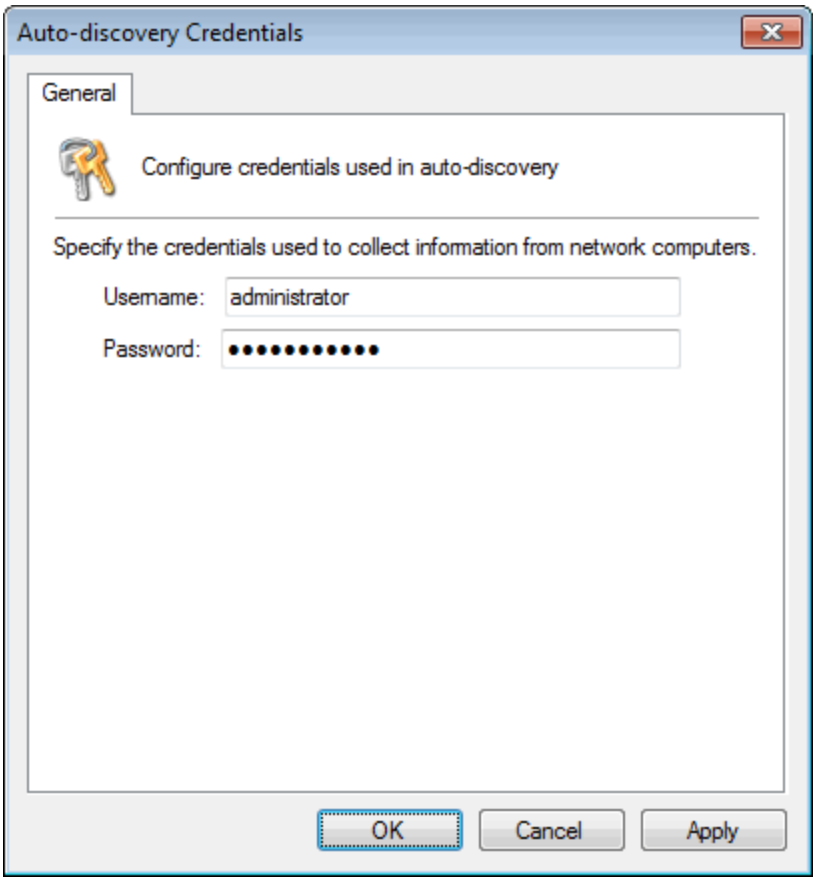
Las credenciales de detección automática son utilizadas por GFI EventsManager para iniciar sesión en los equipos de destino y recopilar información al realizar una búsqueda automática de orígenes de eventos. Para configurar las credenciales de detección automática:



Captura de pantalla 195: Configurar credenciales de detección automática

1. En la ficha **Configuration > Options**, amplíe el nodo **Console Security and Audit Options**.

2. Haga clic con el botón secundario en **Auto-discovery credentials** y seleccione **Edit auto-discovery credentials**.



Captura de pantalla 196: Especifique las credenciales de detección automática

3. Ingrese un nombre de usuario y una contraseña válidos.

4. Haga clic en **Apply** y **OK**.

14 Mantenimiento de base de datos

En este capítulo, se proporciona información sobre el sistema de almacenamiento que utiliza GFI EventsManager para almacenar los eventos procesados. Este sistema permite una gran escalabilidad con sus rápidas capacidades de lectura/escritura, incluso cuando se procesan grandes volúmenes de datos. Para ayudarlo a mantener el back-end de su base de datos, GFI EventsManager le proporciona opciones dedicadas de tareas de mantenimiento.

Las tareas de mantenimiento de bases de datos proporcionan una funcionalidad avanzada para los administradores, lo que les permite:

- Centralizar los eventos que recopilaron otras instancias remotas de GFI EventsManager en un solo back-end de base de datos.
- Optimizar el rendimiento de GFI EventsManager al controlar activamente el crecimiento del back-end de base de datos y, por lo tanto, mantenerlo en buen estado.
- Importar y exportar datos hacia y desde versiones anteriores de GFI EventsManager sin incoherencias en los datos.
- Importar y exportar eventos hacia y desde una carpeta de almacenamiento, de modo que se minimicen las cargas de datos desde la base de datos.

Temas de este capítulo:

14.1 Administrar back-end de base de datos 252

14.2 Crear tareas de mantenimiento 262

14.3 Editar tareas de mantenimiento 292

14.1 Administrar back-end de base de datos

En esta sección, se describe cómo puede administrar fácilmente el back-end de la base de datos a través de la Consola de administración de GFI EventsManager.

Esta sección contiene información acerca de:

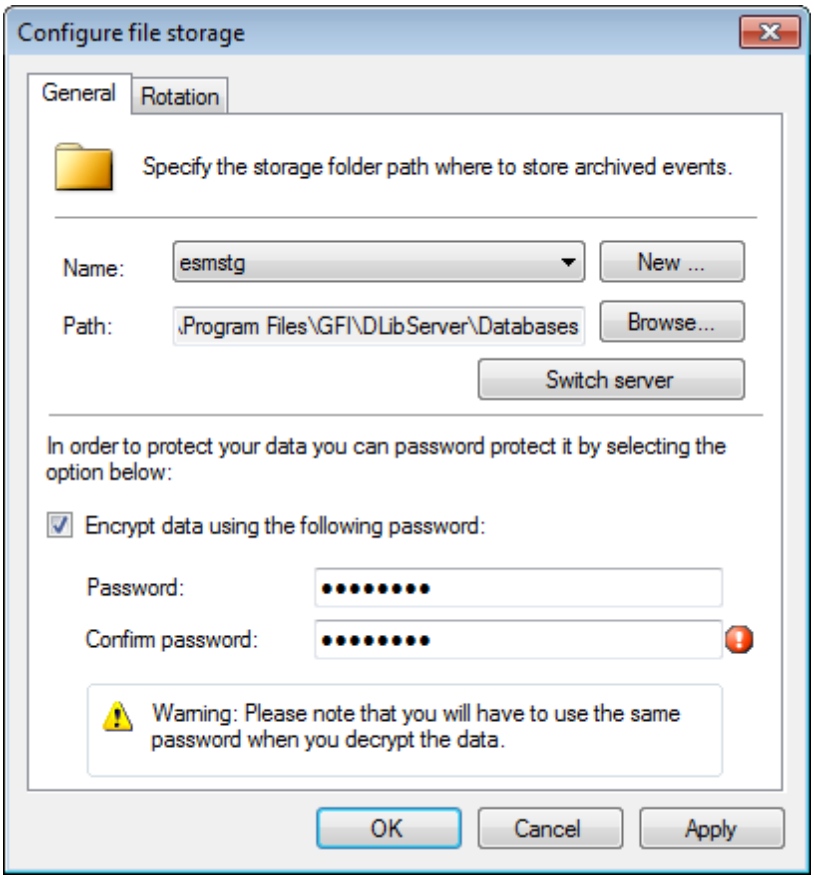
- Crear una nueva base de datos
- Proteger su base de datos
- Habilitar hashing de registro de la base de datos
- Cambiar de base de datos
- Configurar opciones de rotación de bases de datos

14.1.1 Crear una nueva base de datos

GFI EventsManager le permite tener varias bases de datos para almacenar los registros de eventos procesados. Mediante el Explorador de eventos, la ficha Reporting y otras ubicaciones, puede cambiar fácilmente de una base de datos a otra, lo que le permite ver eventos o generar informes desde varias bases de datos. Se pueden proteger con una capa adicional las bases de datos mediante el cifrado con una contraseña.

Para crear una nueva base de datos:

1. En la ficha **Configuration > Options > Configurations**, haga clic con el botón secundario en **File Storage** y seleccione **Configure file storage…**.



Captura de pantalla 197: Cuadro de diálogo File storage system

2. Haga clic en **New** y escriba el nombre de la nueva base de datos. Haga clic en **OK** para cerrar el cuadro de diálogo Create new database.

3. Haga clic en **Browse** para seleccionar una ubicación distinta del almacén de base de datos predeterminado.

4. (Opcional) Seleccione **Encrypt data using the following password** y especifique la contraseña de cifrado que se utiliza para proteger la información en la nueva base de datos.

Nota

Indica que las contraseñas especificadas no coinciden.

5. Haga clic en **Apply** y **OK**.

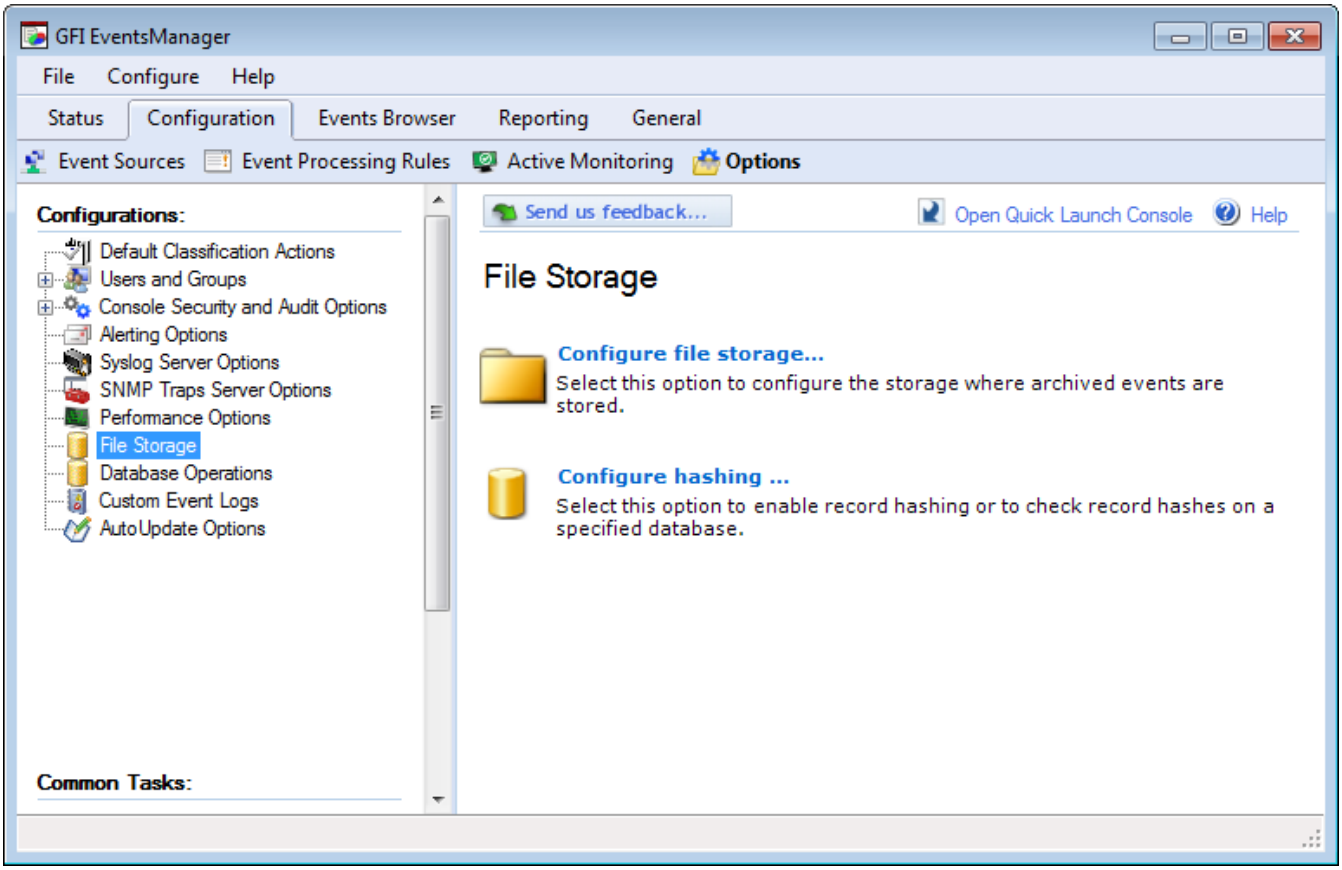
14.1.2 Proteger su base de datos

GFI EventsManager le permite proteger su base de datos con una clave de cifrado. Cifrar la base de datos impide que el personal no autorizado pueda acceder a los registros de eventos.

Importante

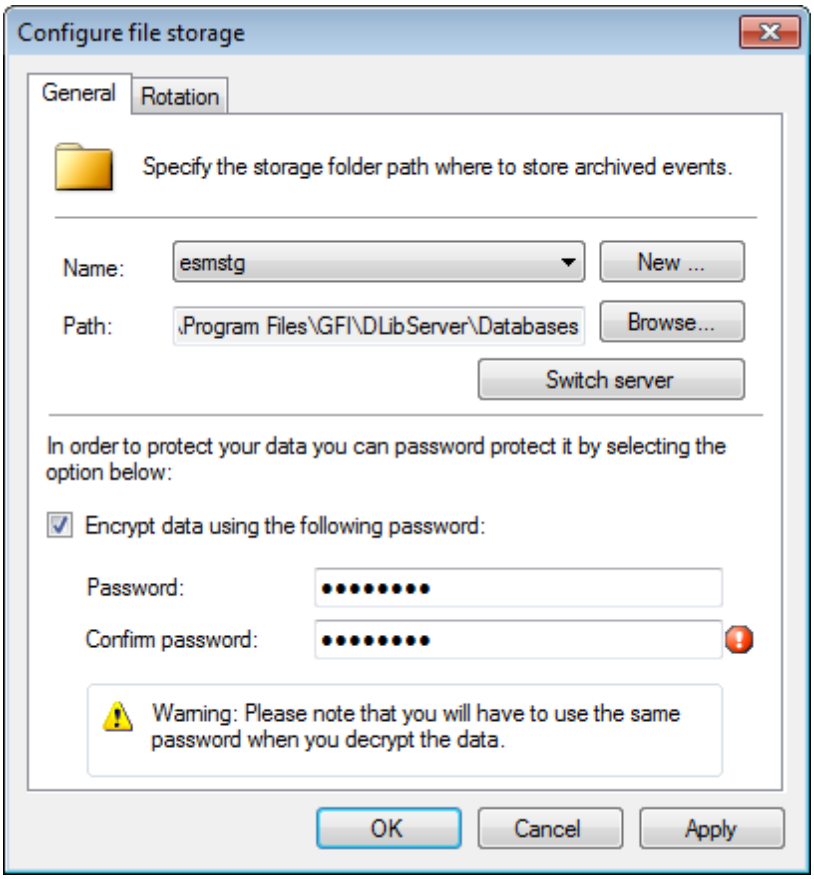
Cifrar la base de datos genera que el **Monitor de estado** y el **Explorador de eventos** dejen de ver la información confidencial.

Para cifrar el back-end de la base de datos:



Captura de pantalla 198: Editar configuración de almacenamiento de archivos

1. Haga clic en la ficha **Configuration > Options**, haga clic con el botón secundario en **File Storage** y seleccione **Configure file storage...**.



Captura de pantalla 199: Habilitar el cifrado

2. En la ficha **General**, seleccione **Encrypt data using the following password** para activar el cifrado.

3. Especifique la contraseña y la contraseña de confirmación.

> **Nota**
>
> Indica que las contraseñas especificadas no coinciden.

4. Haga clic en **Apply** y **OK**.

> **Nota**
>
> La base de datos activa (la base de datos que está utilizando actualmente) no se puede cifrar desde este cuadro de diálogo. Solamente las bases de datos nuevas o sin conexión se pueden cifrar desde aquí. Para cifrar la base de datos activa, utilice la herramienta CMD provista: **esmdlibm.exe**. Para obtener más información, consulte Usar Esmdlibm.exe.

14.1.3 Hashing de registro de base de datos

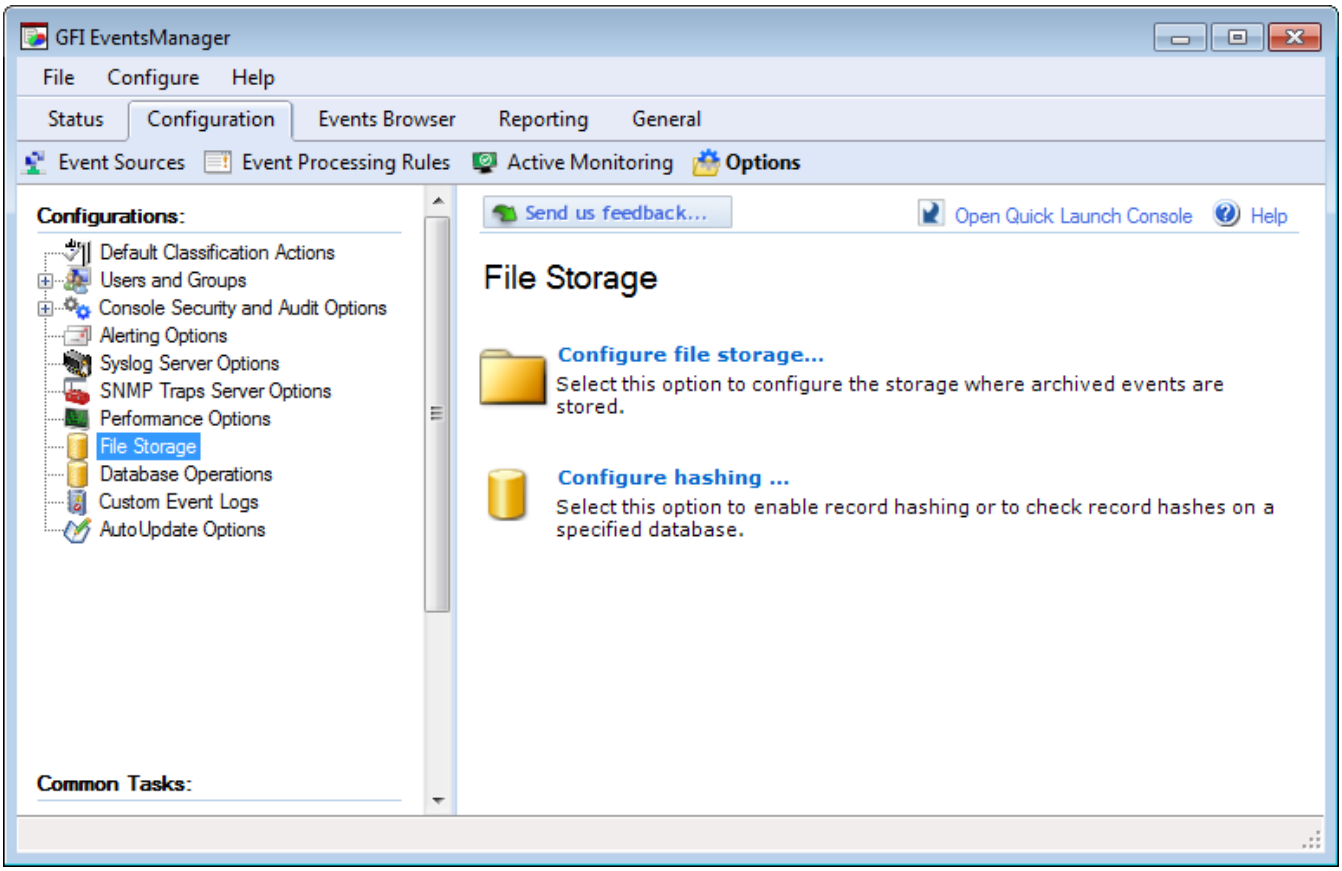
Para proteger sus datos más eficientemente, GFI EventsManager le proporciona capacidades de hashing de registros. El hashing de nuevos registros es un método que se utiliza para asegurar que los datos en sus bases de datos no se modifiquen. Cuando se habilita el hashing de registros, se crea un hash para cada registro recopilado a la hora de recopilación. El hash se diseña en base a los datos

contenidos en el propio registro de eventos y se crea no bien se recopila el registro de eventos para asegurar que sea la versión original. Cuando los datos de un registro con hash se modifican (incluso el carácter de una palabra), el valor del hash cambia, lo cual indica que alguien podría estar alterando los documentos almacenados.

Importante

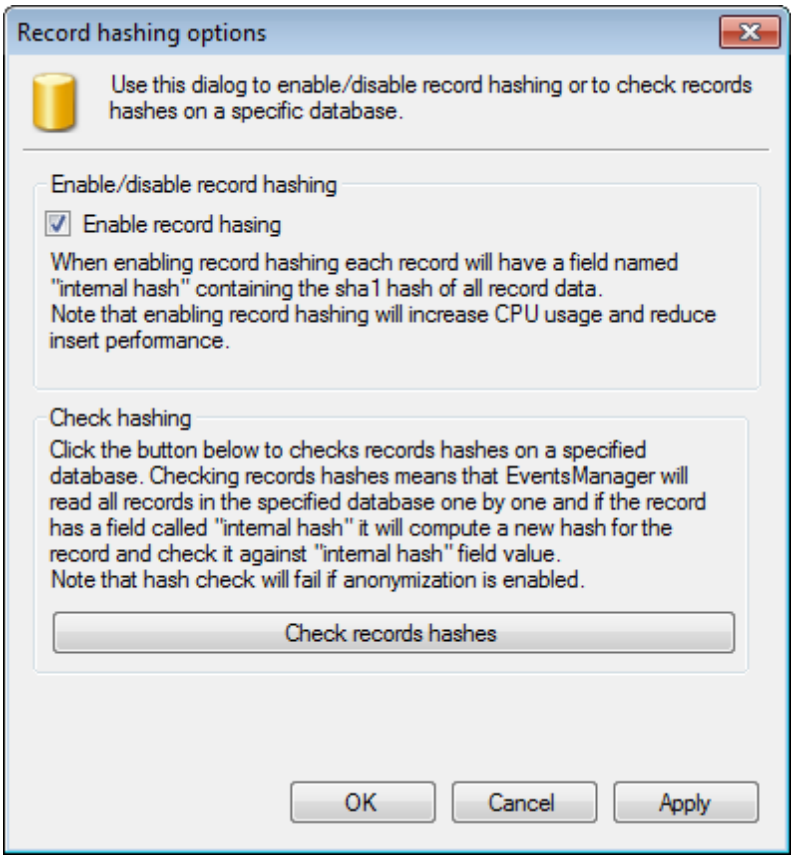
El hashing fallará si la anonimización está habilitada.

Para configurar el proceso de hashing:



Captura de pantalla 200: Activar o desactivar hashing de registros

1. En la ficha **Configuration > Options > Configurations**, haga clic en **File Storage > Configure hashing...**.


Record hashing options
Use this dialog to enable/disable record hashing or to check records hashes on a specific database.
Enable/disable record hashing
Enable record hasing
When enabling record hashing each record will have a field named "internal hash" containing the sha1 hash of all record data.
Note that enabling record hashing will increase CPU usage and reduce insert performance.
Check hashing
Click the button below to checks records hashes on a specified database. Checking records hashes means that EventsManager will read all records in the specified database one by one and if the record has a field called "internal hash" it will compute a new hash for the record and check it against "internal hash" field value.
Note that hash check will fail if anonymization is enabled.
Check records hashes
OK
Cancel
Apply

Captura de pantalla 201: Cuadro de diálogo Record hashing

2. Marque o desmarque la opción **Enable record hashing** para activar o desactivar las funciones de hashing.

3. Haga clic en **Check records hashes** para ejecutar comprobaciones de hash en la base de datos seleccionada. Seleccione una base de datos de la lista y haga clic en **OK** para iniciar la comprobación.

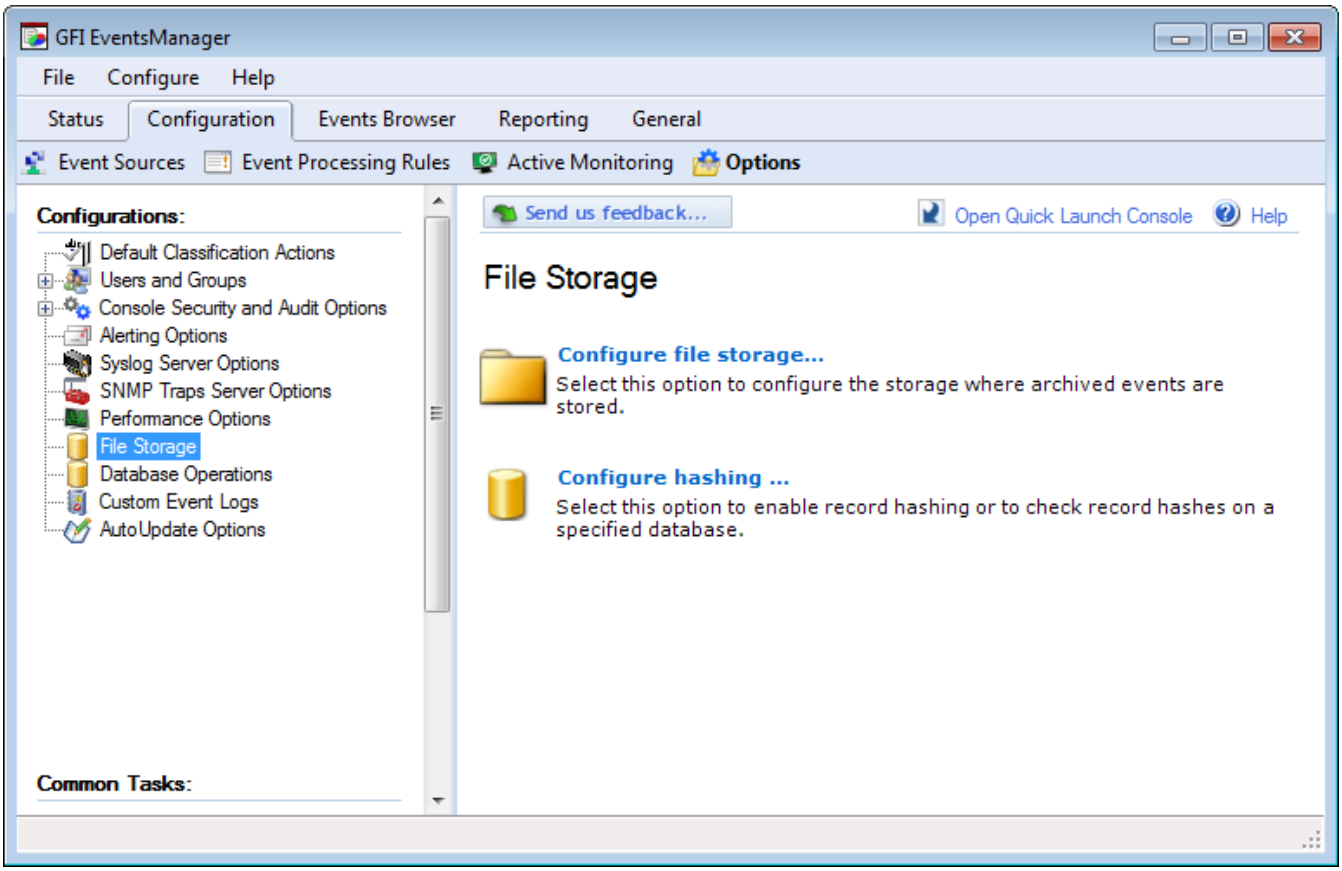
4. Haga clic en **Apply** y **OK**.

14.1.4 Cambiar de base de datos de almacenamiento de archivos

GFI EventsManager le permite utilizar varias bases de datos, almacenadas en diferentes lugares en el mismo equipo o en cualquier equipo remoto dentro de su LAN.

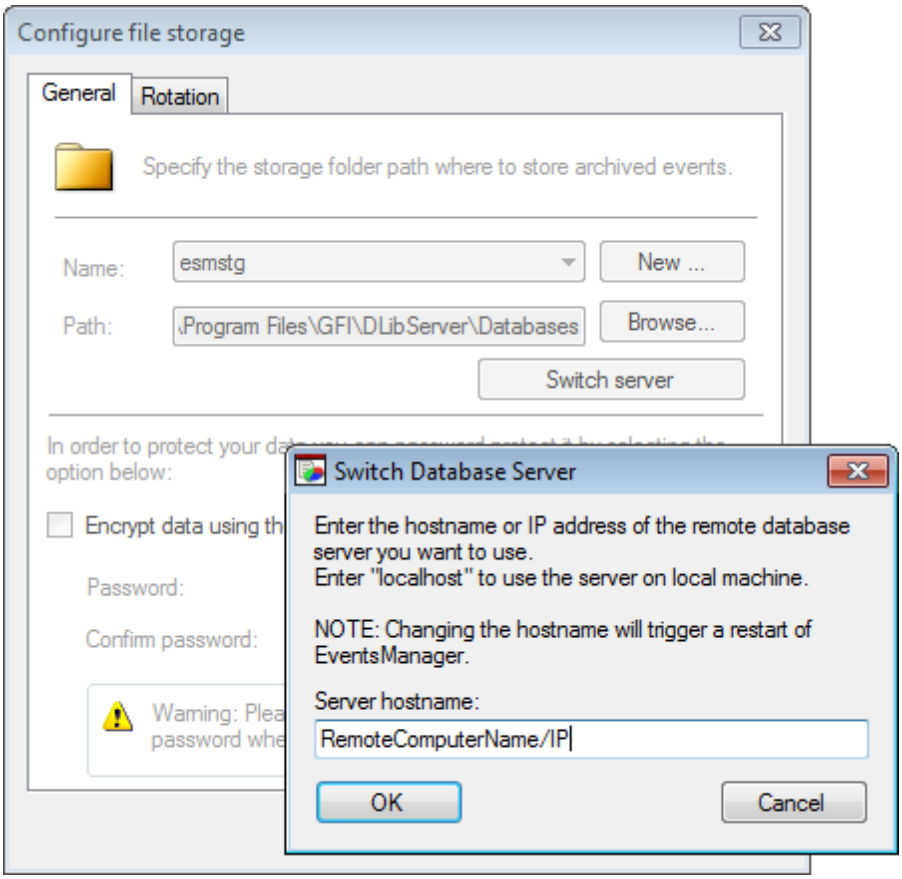
Para cambiar de base de datos:

1. Haga clic en la ficha **Configuration > Options**.



Captura de pantalla 202: Ficha Options

2. En el panel izquierdo, haga clic con el botón secundario en **File Storage** y seleccione **Configure file storage...**.



3. En el cuadro de diálogo Configure file storage, haga clic en **Switch server**. Se abre el cuadro de diálogo Switch Database Server.

4. En el cuadro de texto **Server hostname**, especifique los valores de **Computer Name** o **IP address** del equipo de la base de datos. Haga clic en **Aceptar**.

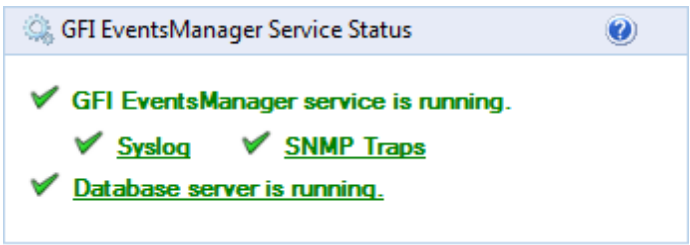
5. Haga clic en **Apply** y **OK**.

Cambiar de base de datos desde el panel

La vista del panel General le permite cambiar de base de datos sin tener que acceder a la ficha de configuración. Esto es útil cuando se comparan registros de eventos o se evalúa la situación general de la administración de eventos en su entorno.

Para cambiar de base de datos desde el panel:

1. Haga clic en **Status > General**.



Captura de pantalla 203: Cambiar de base de datos desde el panel

2. En la sección **GFI EventsManager Service Status**, haga clic en **Database server is running**.

3. En el cuadro de diálogo Configure file storage, haga clic en **Switch server** y especifique los valores de **Name** o **IP address** del servidor de bases de datos. Haga clic en **OK** para aceptar.

4. Haga clic en **Apply** y **OK**.

14.1.5 Configurar opciones de rotación de bases de datos

Cuando se procesan eventos de un gran número de orígenes de eventos, es importante configurar las opciones de rotación de la base de datos. Estas opciones le indican a GFI EventsManager que cambie automáticamente a una nueva base de datos cuando se cumpla una determinada condición. Esto contribuye a mantener un conjunto de bases de datos de tamaño fijo, lo cual permite que GFI EventsManager tenga un mejor rendimiento.

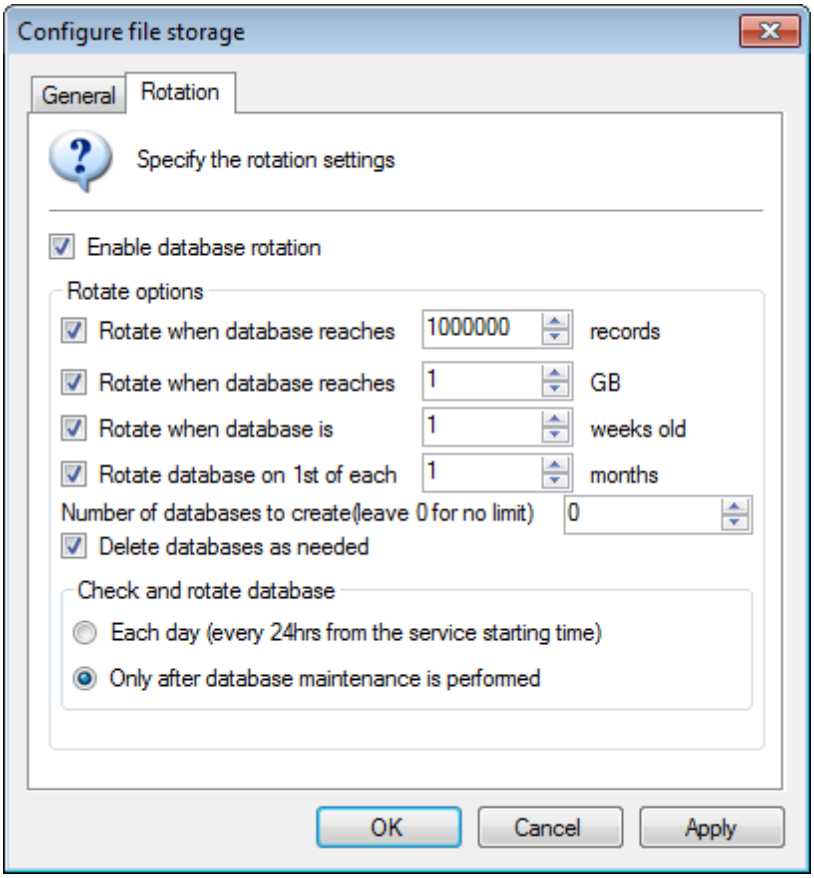
Cuando una base de datos adquiere un tamaño muy grande, las consultas demoran más tiempo en completarse. Por lo tanto, esto afecta el rendimiento de GFI EventsManager de forma negativa.

Por ejemplo, si sus orígenes de eventos normalmente generan una gran cantidad de registros de eventos de tamaño pequeño, permita la rotación de la base de datos cuando se alcance un número máximo de registros. Por otro lado, si sus orígenes de eventos generan registros de eventos de gran tamaño, configure la rotación de la base de datos cuando esta alcance el límite de tamaño.

Para configurar opciones de rotación de la base de datos:

1. Haga clic en la ficha **Configuration** > **Options**.

2. En **Configurations**, haga clic en **File storage > Configure file storage…**.



Captura de pantalla 204: Configurar opciones de rotación de bases de datos

3. Haga clic en **Enable database rotation**.

4. Configure las opciones que se describen a continuación:

Tabla 80: Opciones de rotación de base de datos

Opción	Descripción
Rotate when database reaches {X} Records	Especifique el número de registros que debe contener la base de datos antes de rotar a una nueva. **Nota** Valor mínimo = 1 000 000 registros.
Rotate when database reaches {X} GB	Rotar a una nueva base de datos cuando la base de datos actual alcance el tamaño especificado en GB. **Nota** Valor mínimo = 1 GB.
Rotate when database is {X} weeks old	Rotar la base de datos cuando la base de datos actual sea mayor que el número de semanas especificado. **Nota** Valor mínimo = 1 semana.
Rotate database on 1st of each {X} months	Seleccione esta opción para rotar las bases de datos en el primer día de cada número de meses especificado. Por ejemplo, rote la base de datos en el primer día de cada mes, el primer día cada dos meses o el primer día cada seis meses.
Number of databases to create	Especifique el número máximo de bases de datos que GFI EventsManager puede crear. Deje el valor en **0** para que se pueda crear un número ilimitado de bases de datos.
Delete database as needed	Seleccione esta opción para que, cuando se alcance el número máximo de bases de datos, GFI EventsManager elimine automáticamente la base de datos más antigua para liberar espacio para las nuevas.
Each day (every 24hrs from the service starting time)	Seleccione esta opción para crear y utilizar una nueva base de datos cada 24 horas. Se calculan 24 horas desde el momento en que se inicia el servicio de GFI EventsManager.
Only after database maintenance is performed	Se crea y usa una nueva base de datos después de que una base de datos existente lleve a cabo operaciones de mantenimiento.

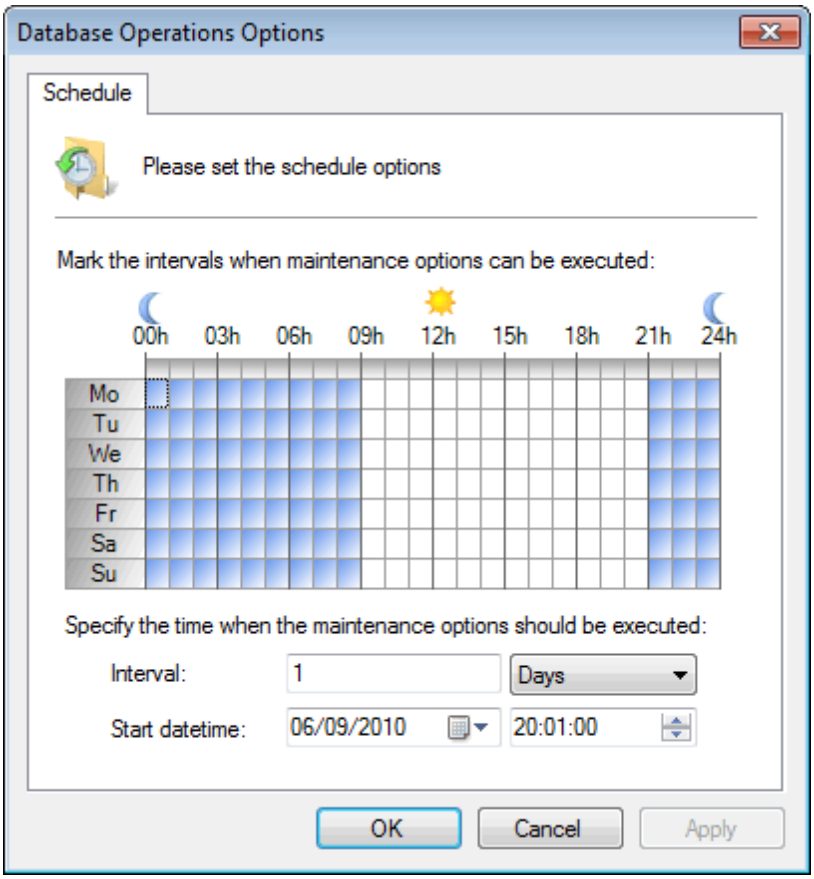
5. Haga clic en **Apply** y **OK**.

14.1.6 Configurar operaciones de base de datos

Para configurar operaciones de base de datos:

1. Haga clic en la ficha **Configuration** > **Options**.

2. En **Configurations**, haga clic con el botón secundario en **Database Operations** y seleccione **Properties**.



Captura de pantalla 205: Cuadro de diálogo Database Operations Options

3. Configure las opciones en las fichas que se describen a continuación:

Tabla 81: Configurar operaciones de base de datos

Ficha	Descripción
General	Especifique el identificador único por el cual esta instancia de GFI EventsManager se identificará en la red. Este identificador se utiliza como parte del nombre de archivo de exportación durante las operaciones de exportación de archivos.
Schedule	A través de la ficha Schedule, especifique: » Las horas del día durante las cuales se pueden ejecutar las tareas de mantenimiento. » El intervalo en horas/días en el que se ejecutarán las tareas de mantenimiento. » La fecha/hora programada durante la cual se iniciará la ejecución de las tareas de mantenimiento.

4. Haga clic en **Apply** y **OK**.

Nota

También se pueden modificar las opciones de programación en la ficha **Configuration > Options > Actions** al hacer clic en **Edit schedule options...**.

14.2 Crear tareas de mantenimiento

Con GFI EventsManager, usted puede programar las tareas de mantenimiento para que se ejecuten en un día determinado, a una hora determinada y a intervalos determinados. Las operaciones de mantenimiento de bases de datos pueden requerir una alta utilización de los recursos. Esto puede reducir el rendimiento del servidor y de GFI EventsManager. Programe tareas de mantenimiento que

se ejecuten después del horario de oficina para maximizar la disponibilidad de los recursos de sus sistemas y evitar posibles interrupciones en el flujo de trabajo.

GFI EventsManager admite dos tipos de tareas de mantenimiento, las cuales se describen a continuación:

Tabla 82: Tipos de tareas de mantenimiento

Tipo de tarea	Descripción
Import\Export Job	Importar datos de otras instancias de GFI EventsManager y exportarlas de otras instancias de la aplicación. Exportar datos e importarlos en otras instancias como parte del proceso de centralización de datos.
Legacy Import Job	Importar datos de versiones anteriores del producto. Importar datos de bases de datos, archivos heredados y almacenamiento de archivos heredados de Microsoft®SQL Server®. Las tareas de importación compatibles con este tipo de tarea se basan en el tipo de back-end de base de datos de versiones anteriores de GFI EventsManager.

Lea las siguientes secciones para obtener información sobre la creación de las siguientes tareas de mantenimiento:

- Importar desde archivo
- Exportar a un archivo
- Exportar a SQL
- Copiar datos
- Confirmar eliminaciones
- Importar de bases de datos de SQL Server®
- Importar de archivos heredados
- Importar del almacenamiento de archivos heredados

14.2.1 Importar desde archivo

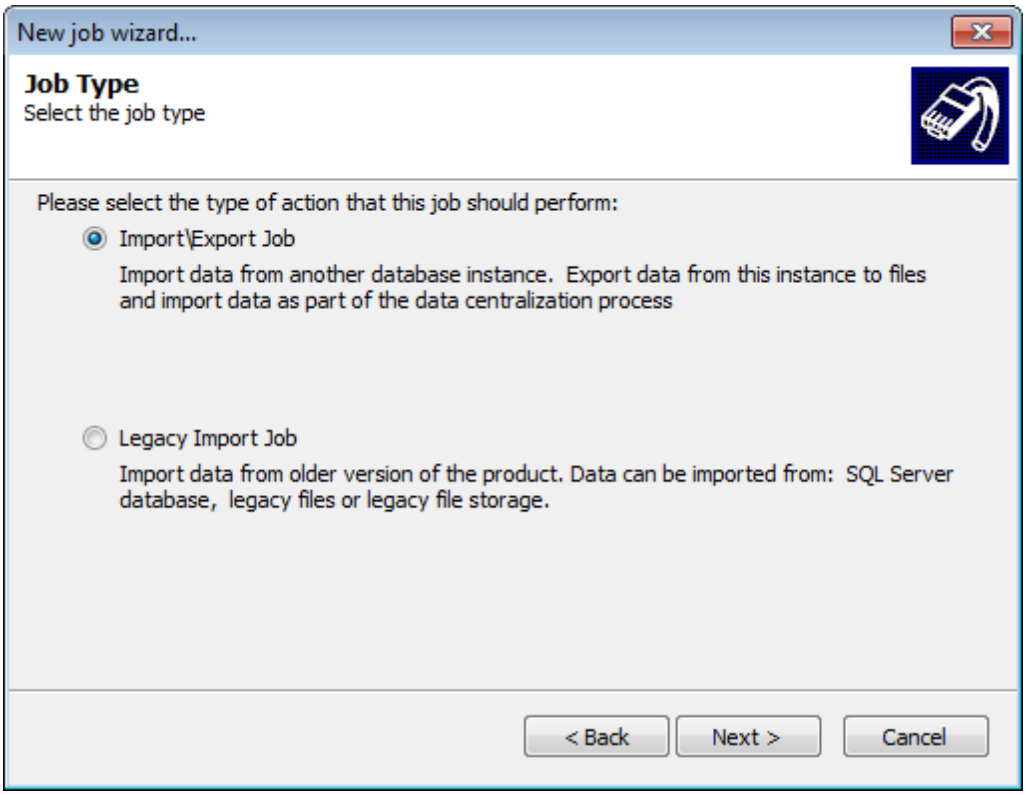
La tarea de importación desde un archivo le permite importar datos que se exportaron anteriormente a un archivo de configuración.

Para crear una tarea de importación desde un archivo:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

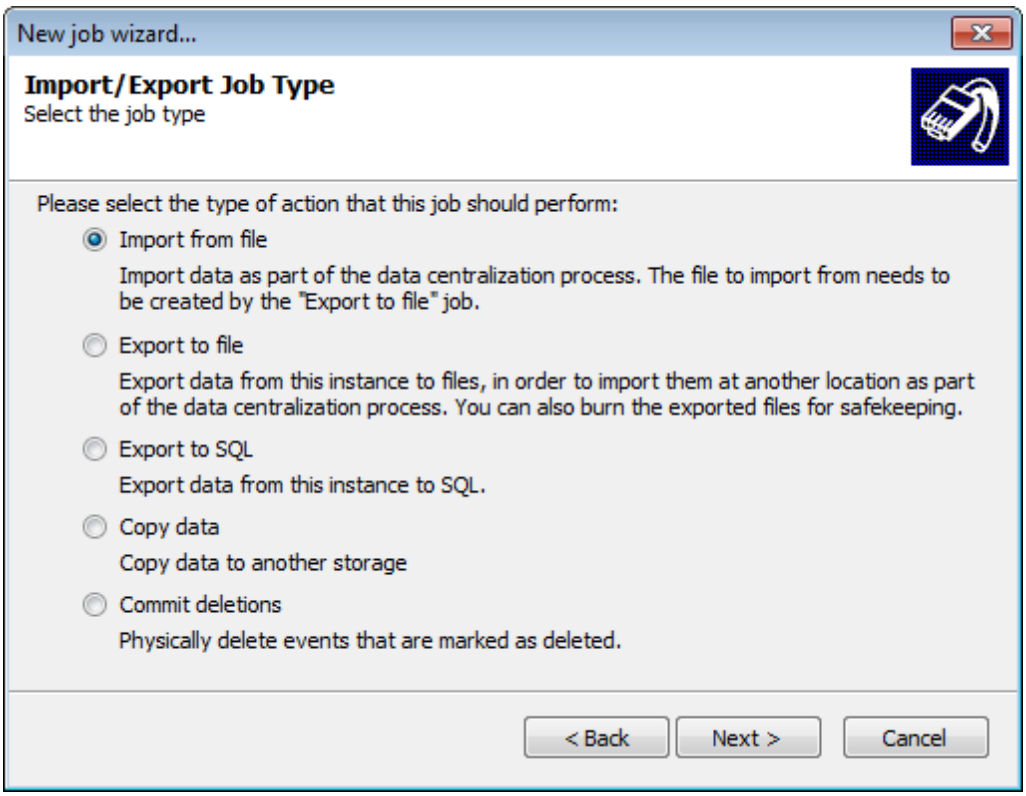
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

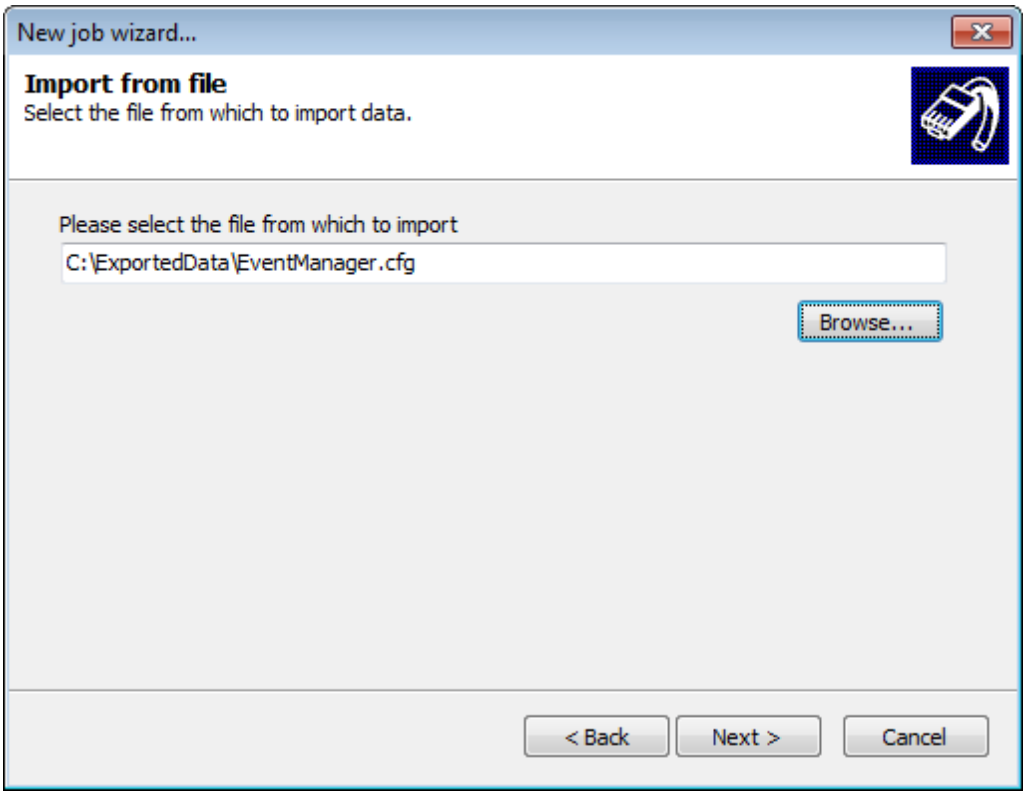
Captura de pantalla 206: Crear tareas de importación/exportación

4. Seleccione **Import/Export Job** y haga clic en **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

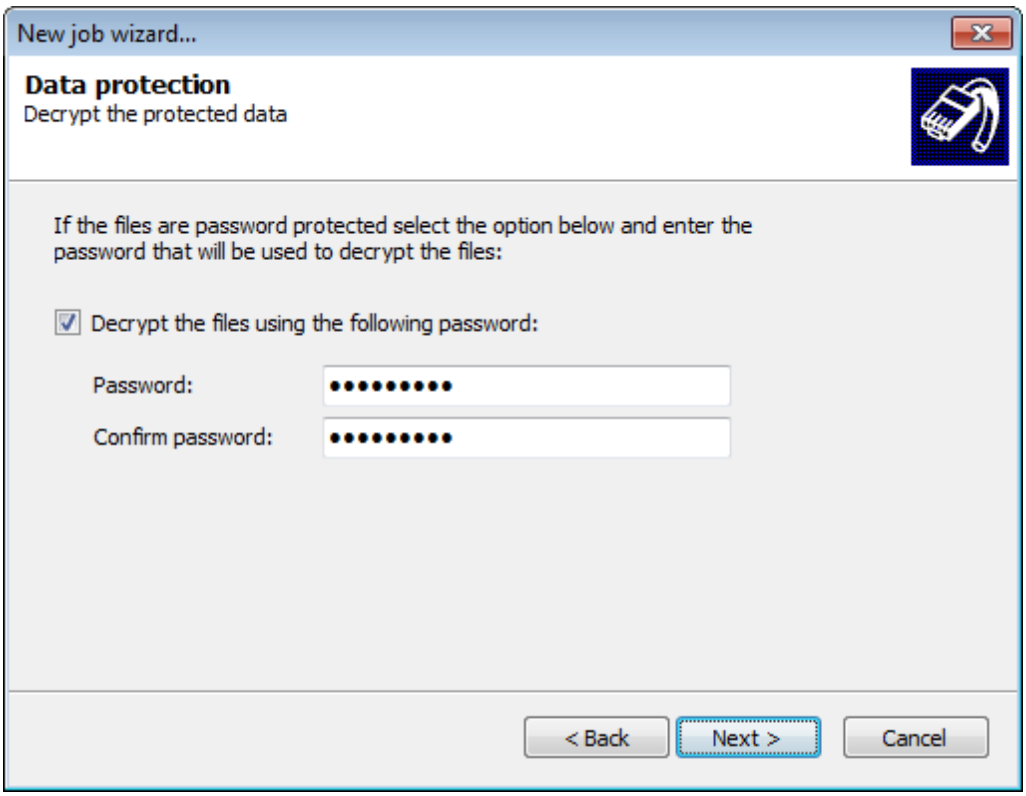
Captura de pantalla 207: Importar desde archivo

5. Seleccione **Import from file** y haga clic en **Next**.



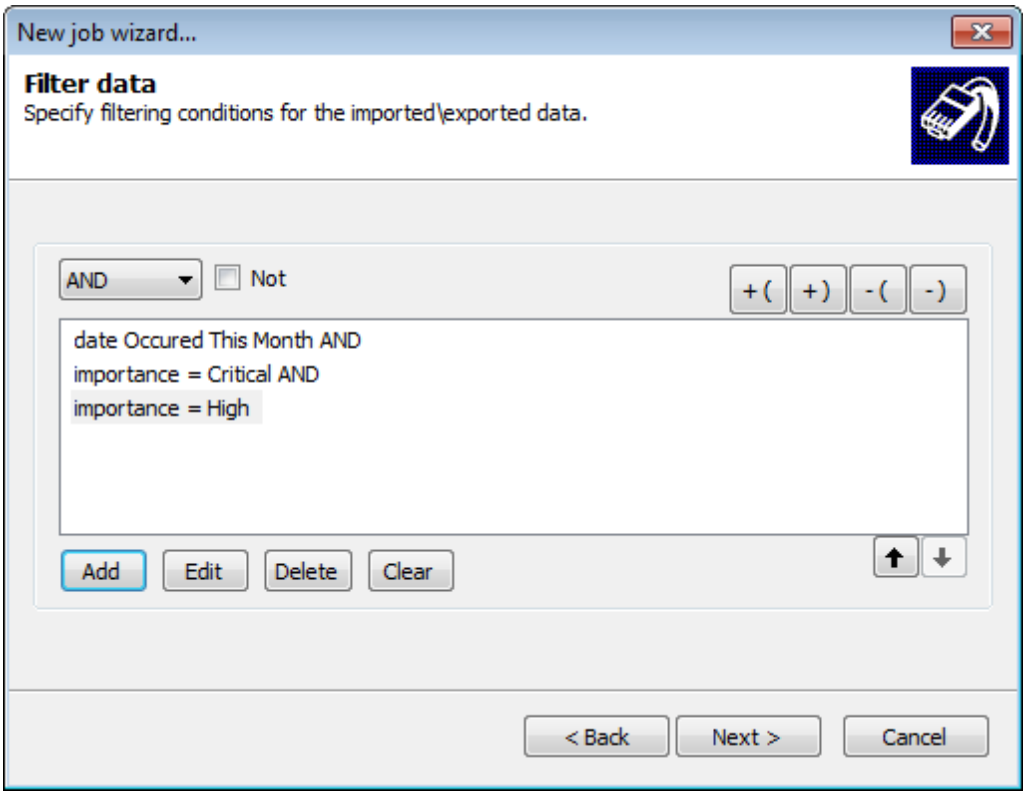
Captura de pantalla 208: Importar desde archivo: Especificar ruta del archivo de importación

6. Especifique la ruta de acceso al archivo de configuración que contiene los datos que desea importar. Opcionalmente, haga clic en **Browse** para buscar la ubicación. Haga clic en **Siguiente**.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Captura de pantalla 209: Descifrar archivos de importación seguros

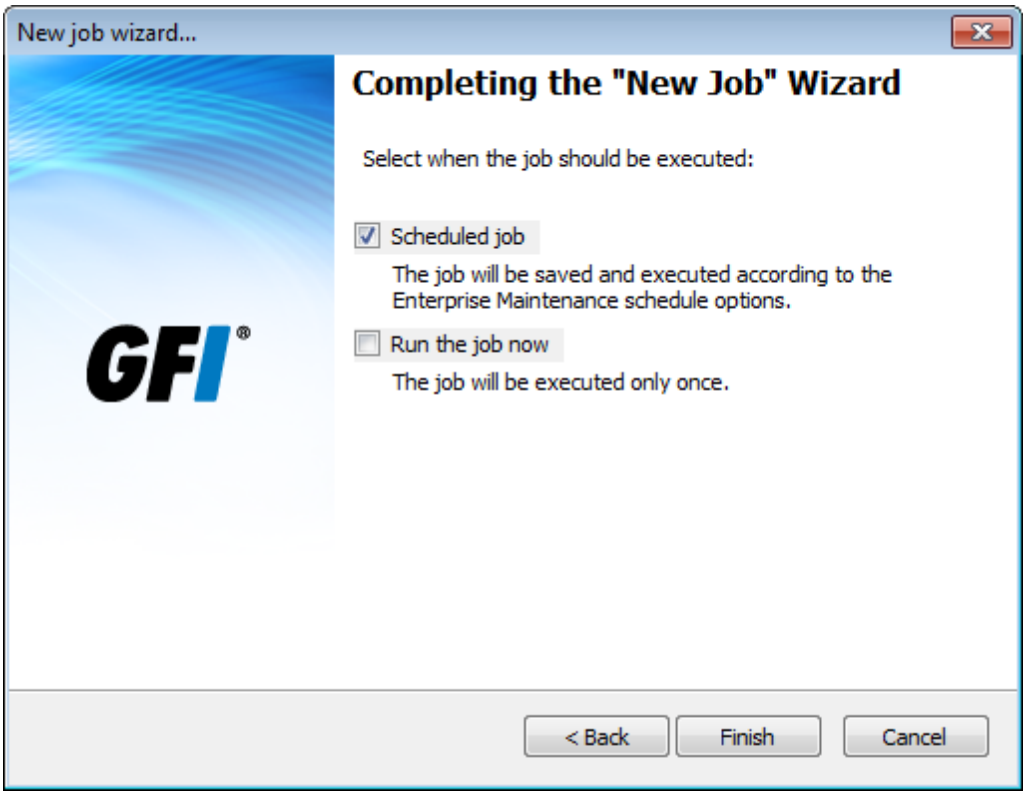
7. (Opcional) Si el archivo que está importando está cifrado, seleccione **Decrypt the files using the following password** y especifique la contraseña que se utiliza para cifrar el archivo. Haga clic en **Siguiente**.



Captura de pantalla 210: Agregar condiciones de filtrado

8. Agregar parámetros de filtrado avanzado para importar solamente datos específicos. Deje en blanco esta opción para importar todos los registros de eventos desde el archivo.

> **Nota**
>
> Para obtener más información, consulte Diseñar restricciones de consultas.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Captura de pantalla 211: Ejecutar opciones de tarea

9. Seleccione cuándo se ejecuta la tarea y haga clic en **Finish**:

Tabla 83: Crear tareas de mantenimiento - Opciones de programación

Opciones	Descripción
Schedule job	La tarea se guardará y se ejecutará de acuerdo con la programación de operaciones de la base de datos.
Run the job now	La tarea se ejecuta inmediatamente. Las tareas no programadas solamente se ejecutan una vez y no pueden ser reutilizadas.

14.2.2 Exportar a un archivo

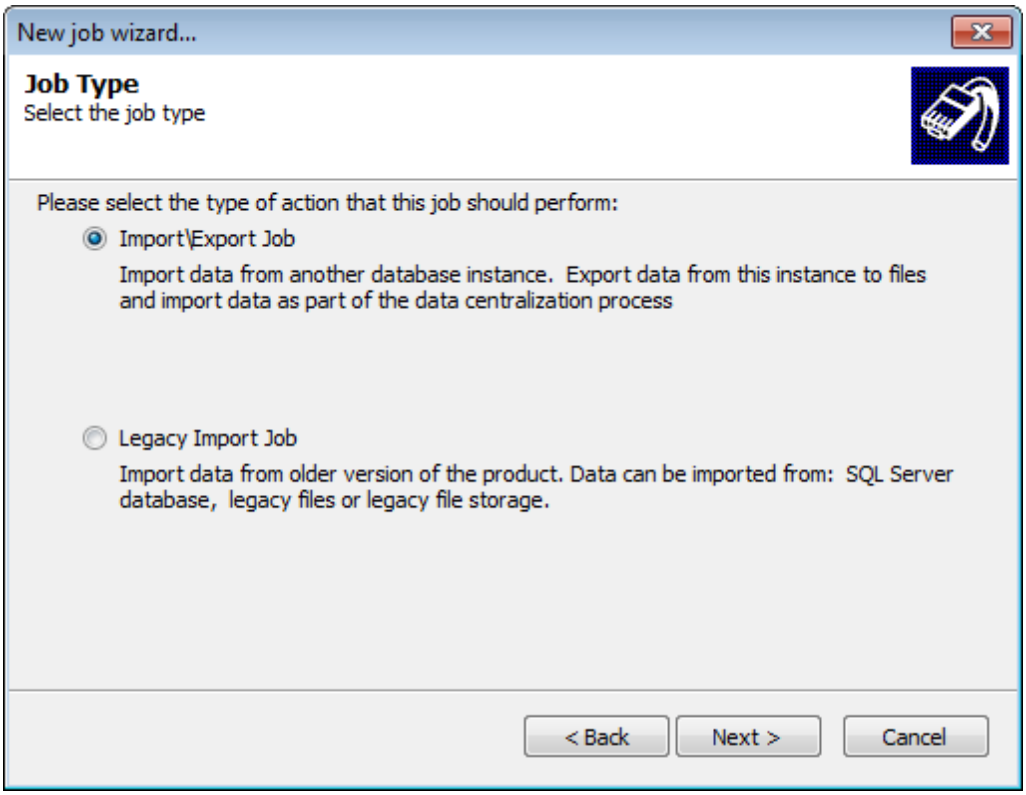
La opción Export to file le permite exportar los parámetros seleccionados a un archivo de configuración que otra instancia o versión de GFI EventsManager puede importar.

Para crear una tarea de exportación a archivo:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

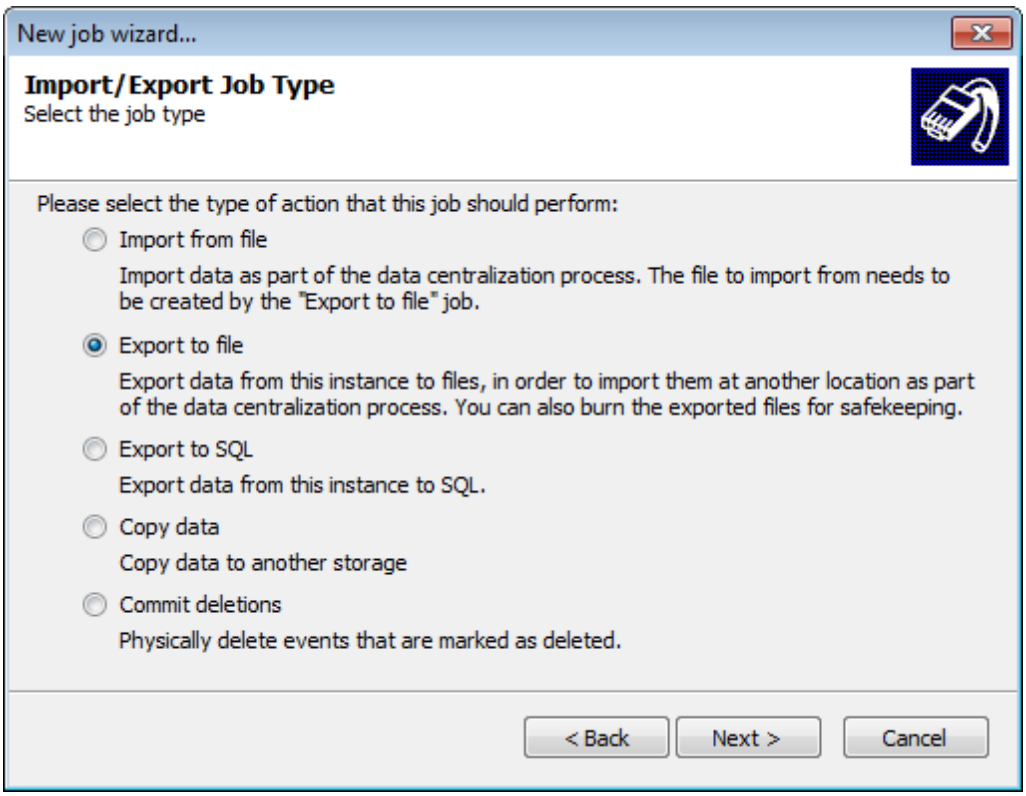
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

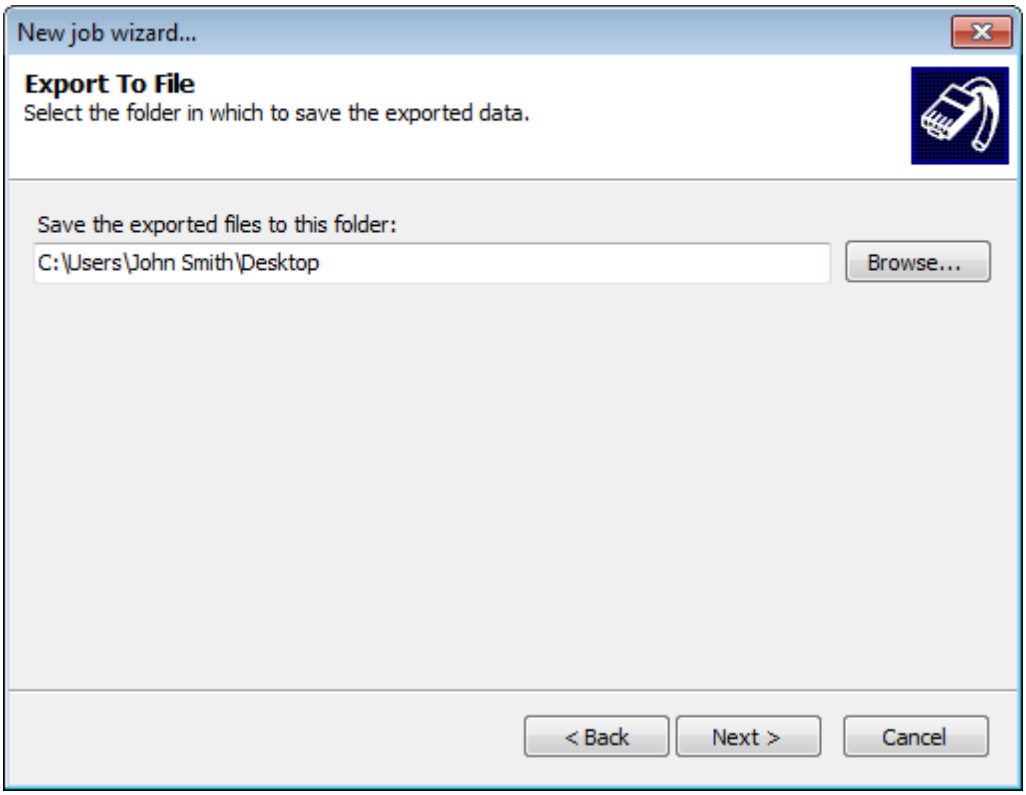
Captura de pantalla 212: Crear tareas de importación/exportación

4. Seleccione **Import/Export Job** y haga clic en **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

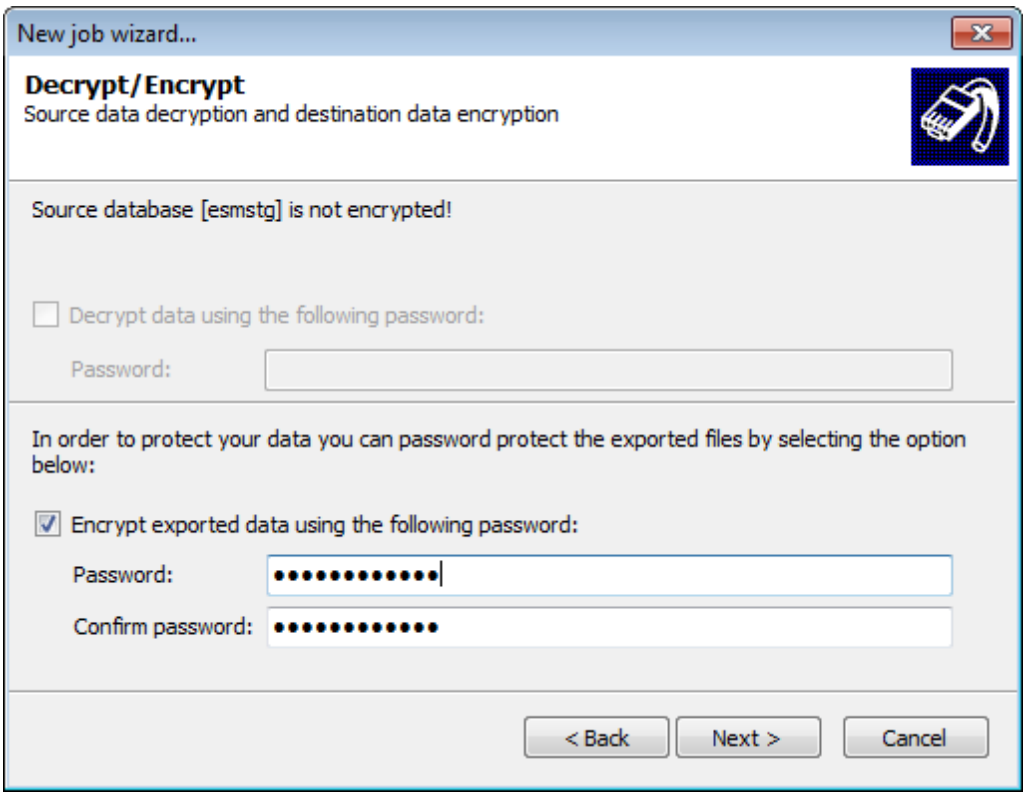
Captura de pantalla 213: Exportar a un archivo

5. Seleccione **Export to file** y haga clic en **Next**.



Captura de pantalla 214:

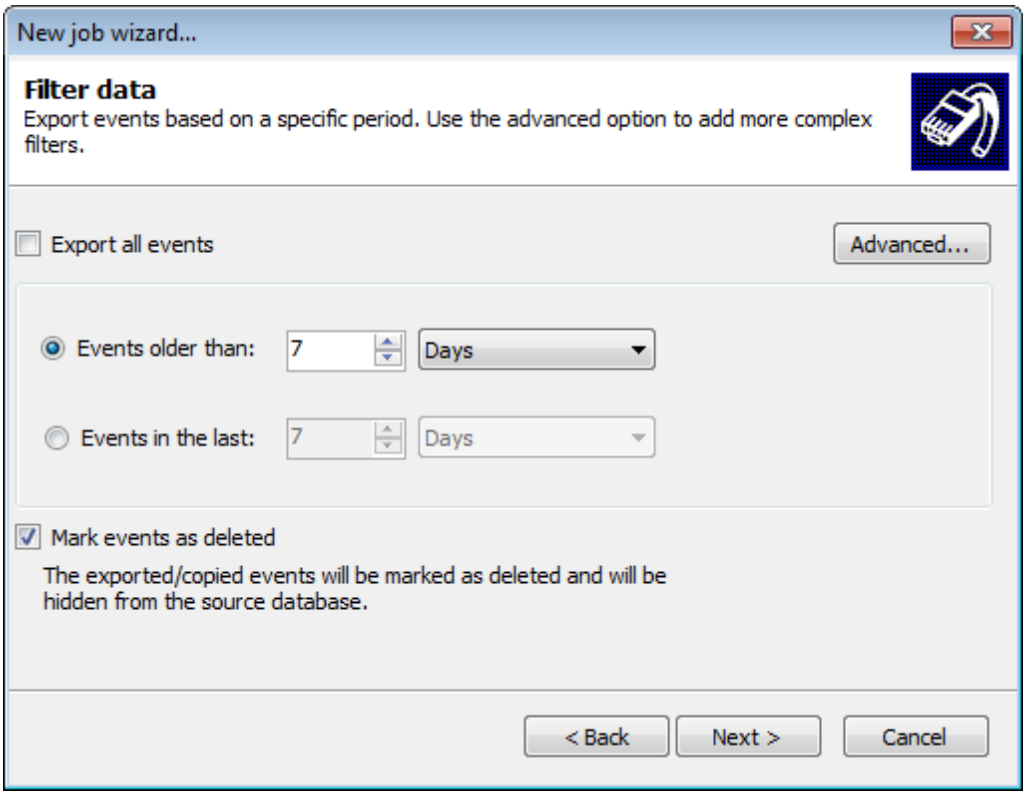
6. Ingrese la ruta de acceso a la carpeta donde se guardan los archivos exportados. O bien, haga clic en **Browse** para buscar la ubicación. Haga clic en **Siguiente**.


New job wizard...
Decrypt/Encrypt
Source data decryption and destination data encryption
Source database [esmstg] is not encrypted!
Decrypt data using the following password:
Password:
In order to protect your data you can password protect the exported files by selecting the option below:
Encrypt exported data using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Captura de pantalla 215: Descifrar/Cifrar datos

7. Si la base de datos de origen (esmstg) está cifrada, seleccione **Decrypt data using the following password** e ingrese la clave de descifrado en el campo **Password**.

8. Para cifrar los datos de exportación, seleccione **Encrypt exported data using the following password** e ingrese una clave de cifrado en los campos **Password** y **Confirm password**. Haga clic en **Siguiente**.

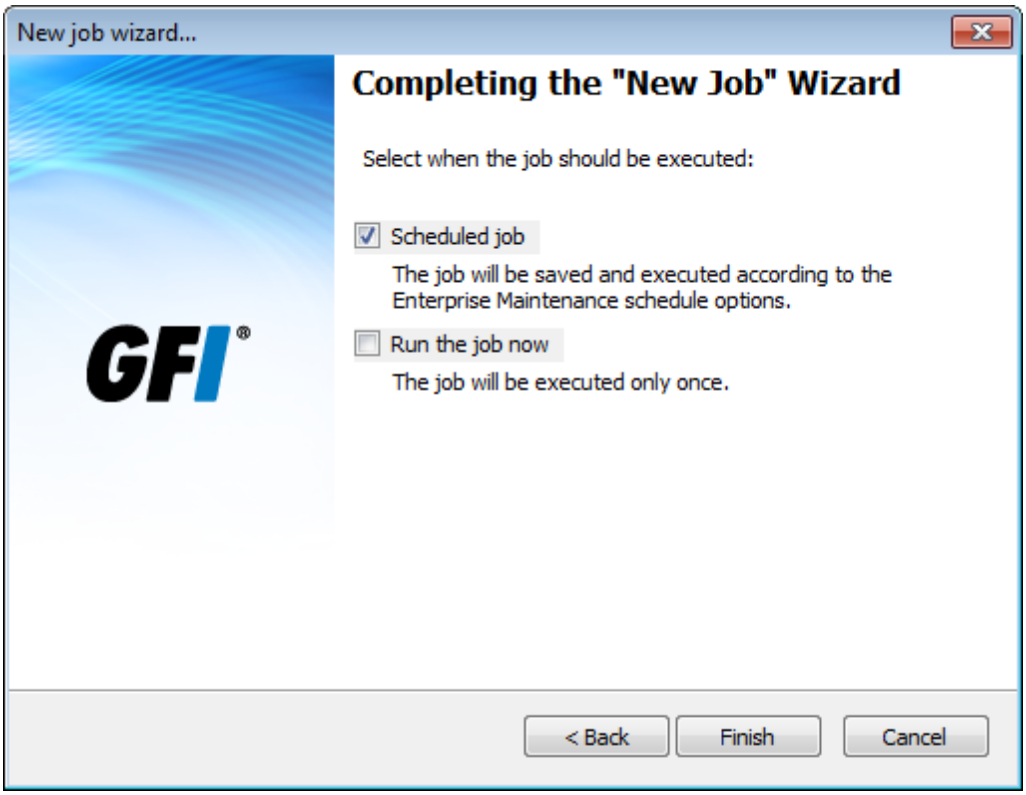

New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Captura de pantalla 216: Filtrar datos exportados

9. Configure las siguientes opciones de filtro y haga clic en **Next**:

Tabla 84: Filtrar datos exportados

Opción	Descripción
Export all events	Exporta todos los eventos de la base de datos.
Events older than	Solamente se exportan los eventos anteriores al número especificado de días/semanas/meses.
Events in the last	Solamente se exportan los eventos que ocurrieron en el último número especificado de días/semanas/meses.
Mark events as deleted	Permite ocultar los eventos de la base de datos de origen después de exportarlos. Para eliminar completamente estos eventos de la base de datos, debe ejecutar una tarea de confirmar eliminaciones. Para obtener más información, consulte Confirmar eliminaciones.
Advanced...	Haga clic en **Advanced...** para iniciar el cuadro de diálogo Advanced Filtering. Le permite configurar parámetros de filtro granulares para exportar únicamente eventos específicos. Para obtener más información, consulte Diseñar restricciones de consulta.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Captura de pantalla 217: Ejecutar opciones de tarea

10. Seleccione cuándo se ejecuta la tarea y haga clic en **Finish**:

Tabla 85: Crear tareas de mantenimiento - Opciones de programación

Opciones	Descripción
Schedule job	La tarea se guardará y se ejecutará de acuerdo con la programación de operaciones de la base de datos.
Run the job now	La tarea se ejecuta inmediatamente. Las tareas no programadas solamente se ejecutan una vez y no pueden ser reutilizadas.

Nombre del archivo de exportación

La convención que utiliza GFI EventsManager para nombrar al archivo de exportación se muestra y se describe a continuación:

```
[ESM ID]_[ID de tarea]_[Fecha inicial]_[Fecha final].EXP
```

Tabla 86: Operaciones de base de datos: Estructura del nombre del archivo de exportación

Sección del nombre	Descripción
ESM ID	Se refiere al identificador único asignado a cada instancia de GFI EventsManager que se ejecuta en la organización.
ID de tarea	Se refiere al identificador único asignado a cada tarea de mantenimiento creada.
Fecha inicial	Se refiere a la fecha del primer evento exportado.
Fecha final	Se refiere a la fecha del último evento exportado.
.EXP	Este es el archivo de extensión que se la asigna a todos los archivos de exportación.

14.2.3 Exportar a SQL

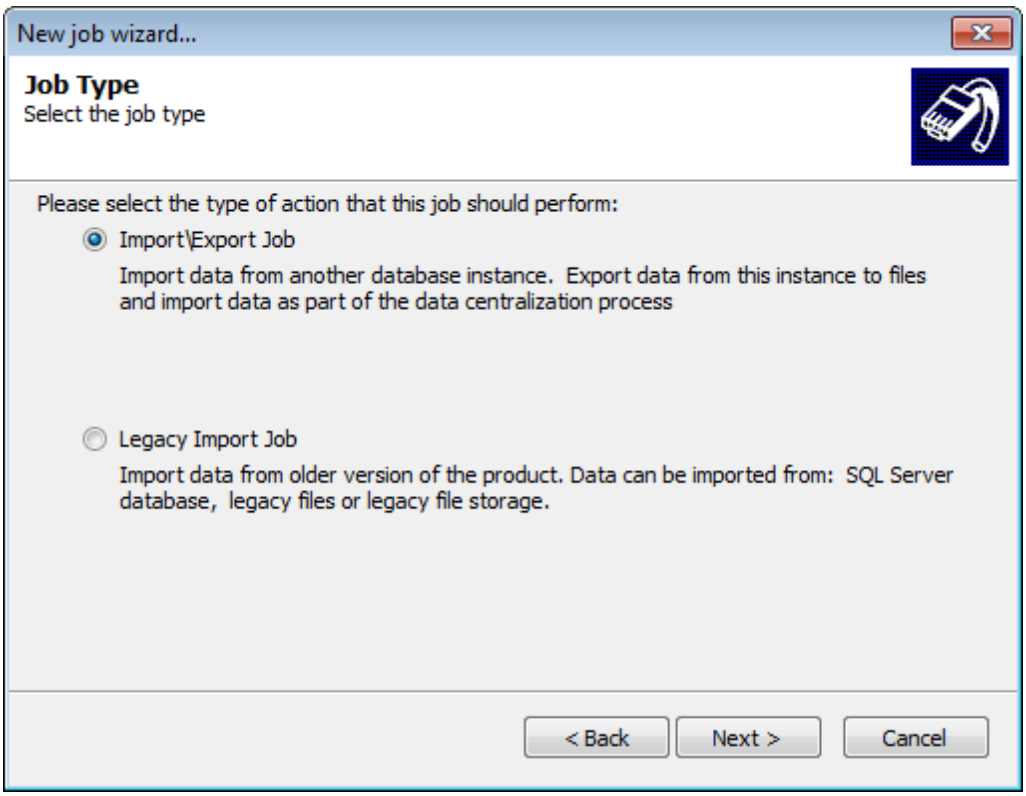
Exportar a SQL le permite exportar documentos directamente a una instancia de SQL Server, a la que se puede llegar por el host de GFI EventsManager.

Para crear una tarea de exportación a SQL:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

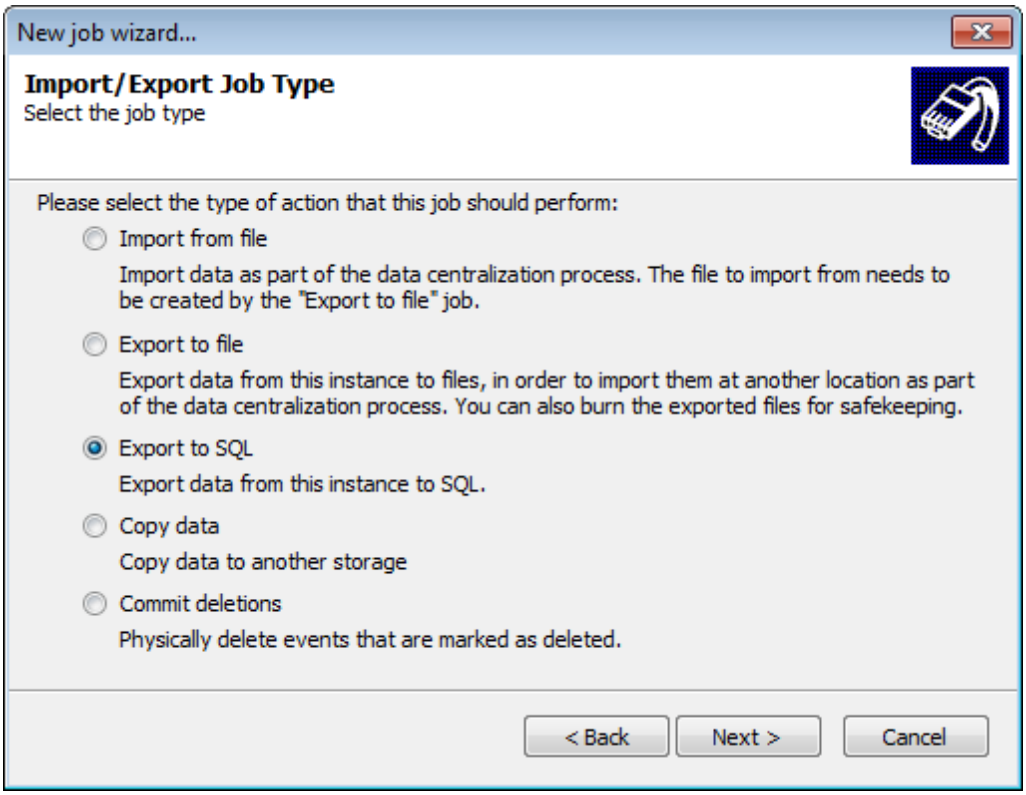
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

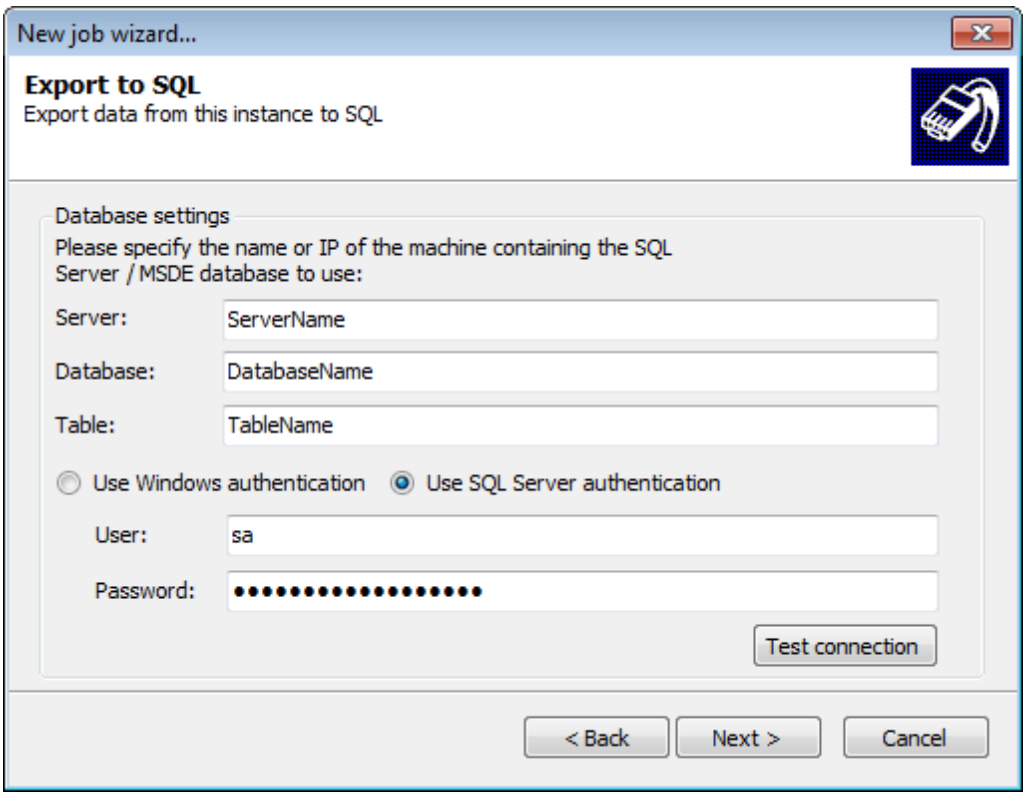
Captura de pantalla 218: Crear tareas de importación/exportación

4. Seleccione **Import/Export Job** y haga clic en **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

Captura de pantalla 219: Exportar a SQL

5. Seleccione **Export to SQL** y haga clic en **Next**.

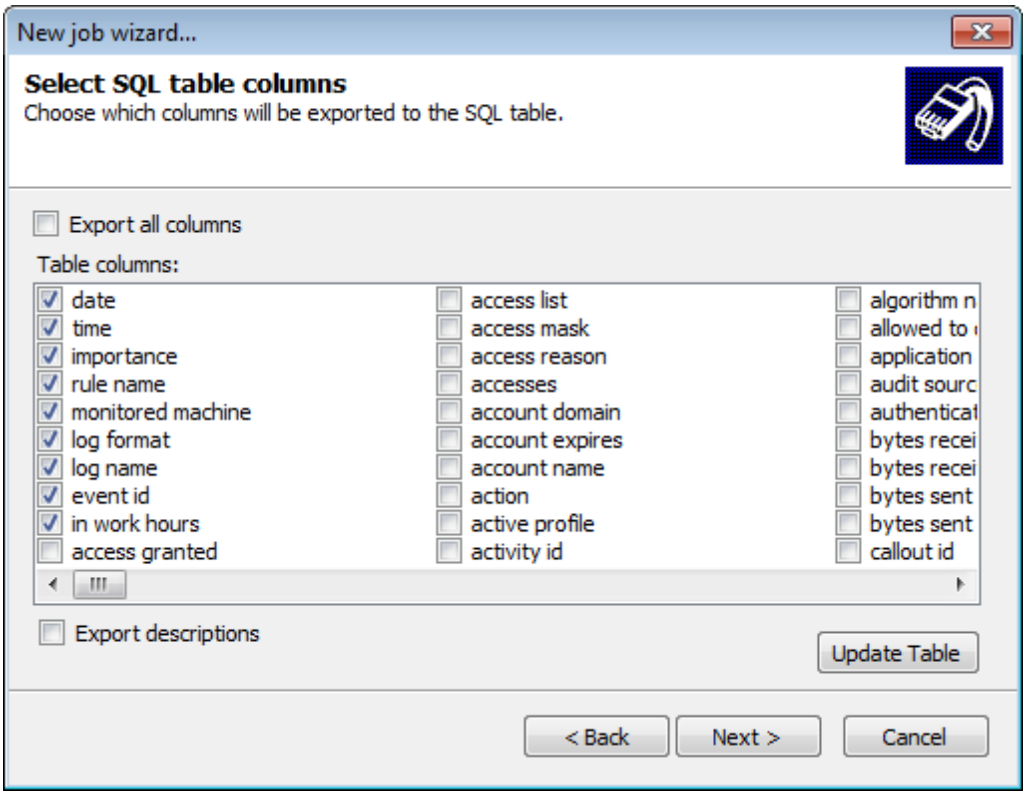


Captura de pantalla 220: Especificar detalles de SQL Server

6. Configure las siguientes opciones de servidor y haga clic en **Next**:

Tabla 87: Exportar a SQL: Opciones del servidor

Opción	Descripción
Server	Escriba el nombre de la máquina que está ejecutando SQL Server.
Base de datos	Escriba el nombre de la base de datos de destino. **Nota** Si la base de datos especificada no existe, GFI EventsManager la crea para usted.
Table	Escriba el nombre de la tabla de destino. **Nota** Si la tabla especificada no existe, GFI EventsManager la crea para usted.
Use Windows authentication	Se usan las mismas credenciales de inicio de sesión que se usan para iniciar sesión en Windows®. SQL Server® debe admitir este tipo de modo de autenticación para poder conectar y copiar la información al servidor.
Use SQL Server authentication	Se usan las credenciales de inicio de sesión configuradas en su SQL Server®. Escriba el nombre de usuario en el campo **User** y la contraseña en el campo **Password**.
Test connection	Haga clic en **Test Connection** para intentar conectarse a SQL Server® con la configuración especificada. **Nota** GFI EventsManager prueba la conexión de forma automática después de que se hace clic en **Next**.

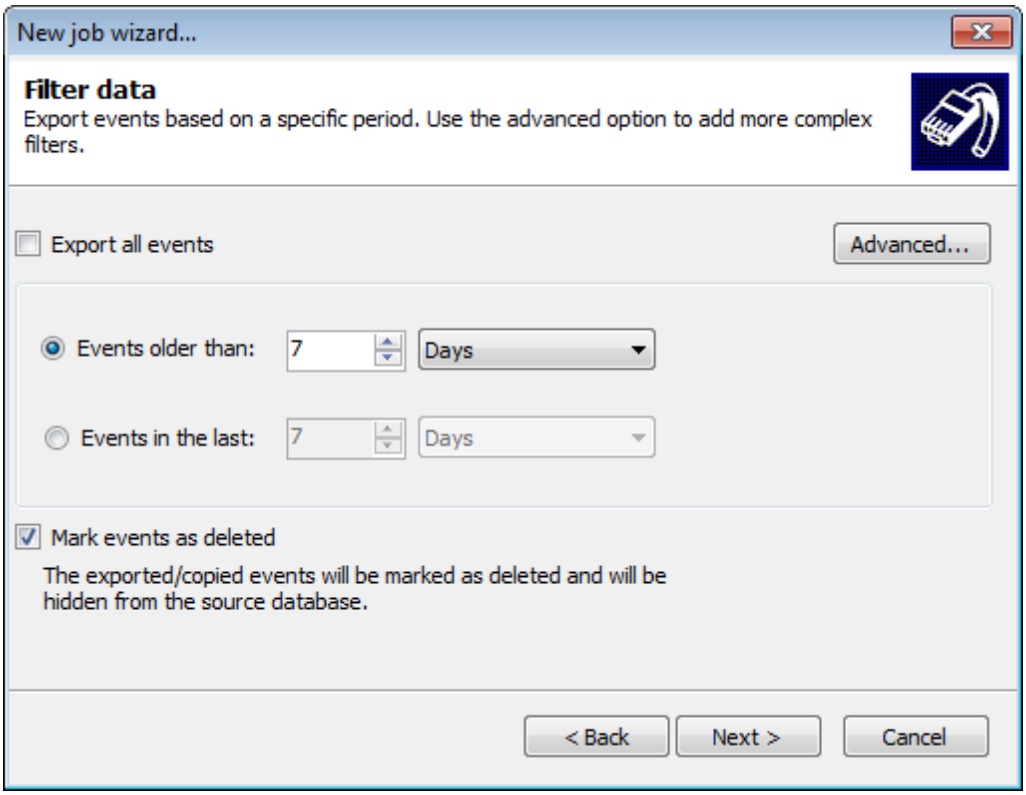


Captura de pantalla 221: Seleccionar columnas que desea exportar

7. Seleccione las columnas que desea exportar y haga clic en **Next**.

Nota

Para exportar todas las columnas, seleccione **Export all columns**.

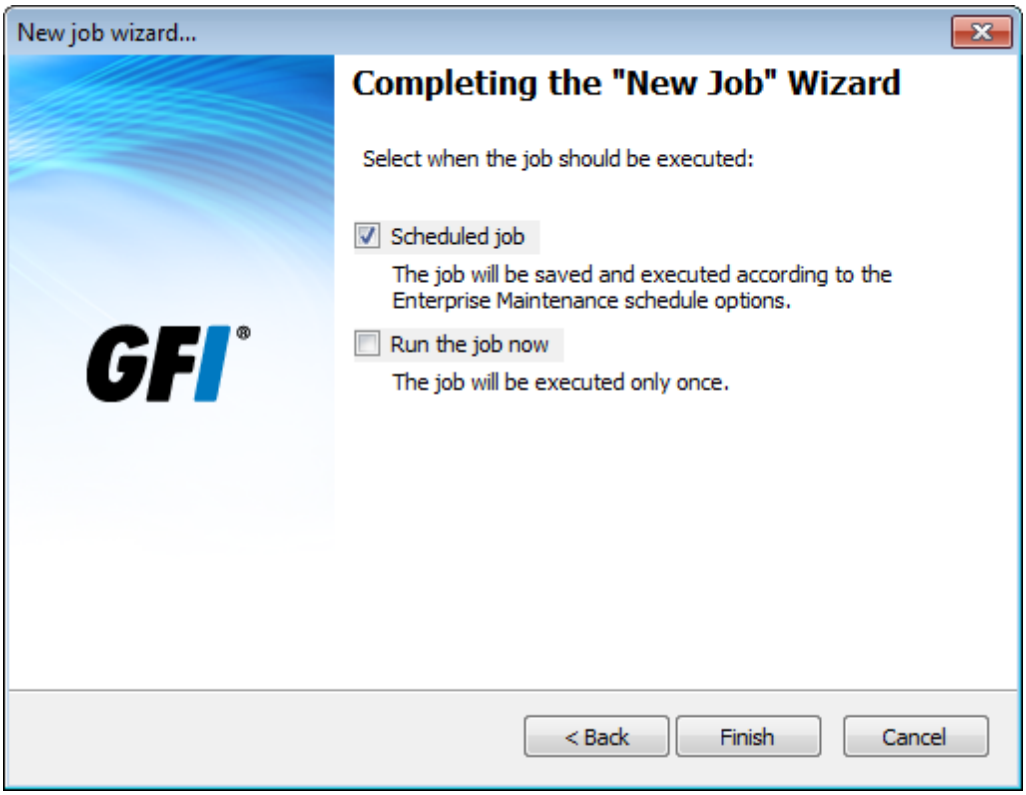

New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Captura de pantalla 222: Filtrar datos exportados

8. Configure las siguientes opciones de filtro y haga clic en **Next**:

Tabla 88: Filtrar datos de exportación

Opción	Descripción
Export all events	Exporta todos los eventos de la base de datos.
Events older than	Solamente se exportan los eventos anteriores al número especificado de días/semanas/meses.
Events in the last	Solamente se exportan los eventos que ocurrieron en el último número especificado de días/semanas/meses.
Mark events as deleted	Permite ocultar los eventos de la base de datos de origen después de exportarlos. Para eliminar completamente estos eventos de la base de datos, debe ejecutar una tarea de confirmar eliminaciones. Para obtener más información, consulte Confirmar eliminaciones.
Advanced...	Haga clic en Advanced... para iniciar el cuadro de diálogo Advanced Filtering. Le permite configurar parámetros de filtro granulares para exportar únicamente eventos específicos. Para obtener más información, consulte Diseñar restricciones de consulta.


New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
< Back
Finish
Cancel

Captura de pantalla 223: Ejecutar opciones de tarea

9. Seleccione cuándo se ejecuta la tarea y haga clic en **Finish**:

Tabla 89: Crear tareas de mantenimiento - Opciones de programación

Opciones	Descripción
Schedule job	La tarea se guardará y se ejecutará de acuerdo con la programación de operaciones de la base de datos.
Run the job now	La tarea se ejecuta inmediatamente. Las tareas no programadas solamente se ejecutan una vez y no pueden ser reutilizadas.

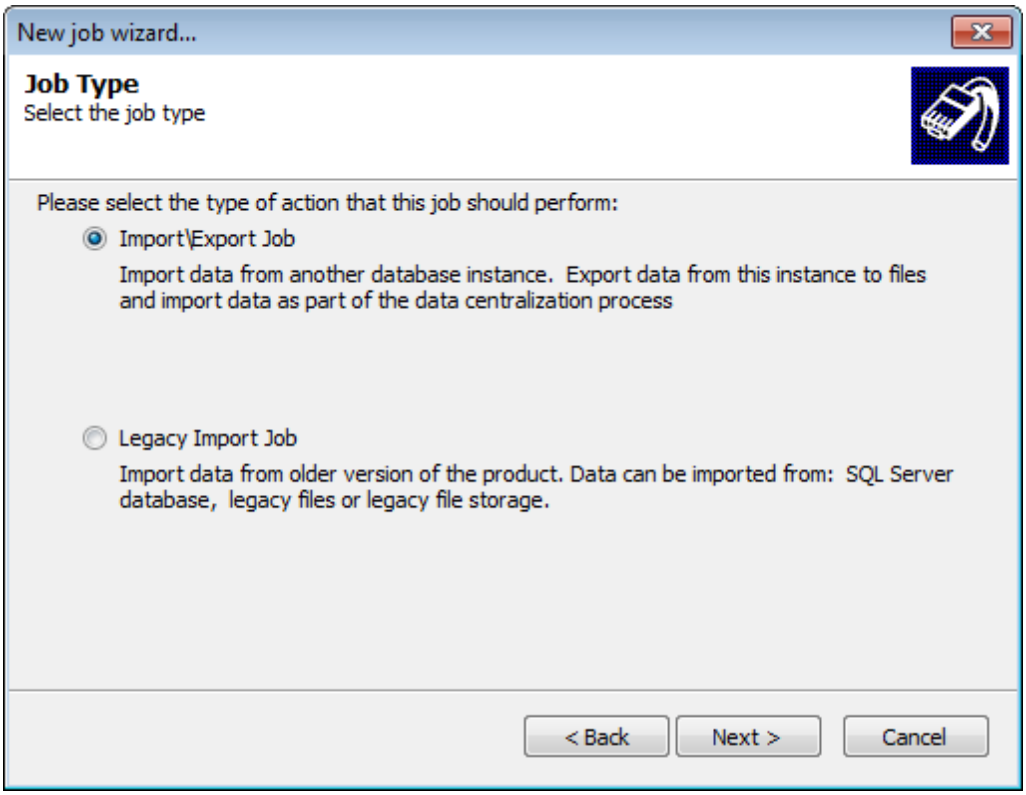
14.2.4 Copiar datos

Para crear tareas de copia de datos:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

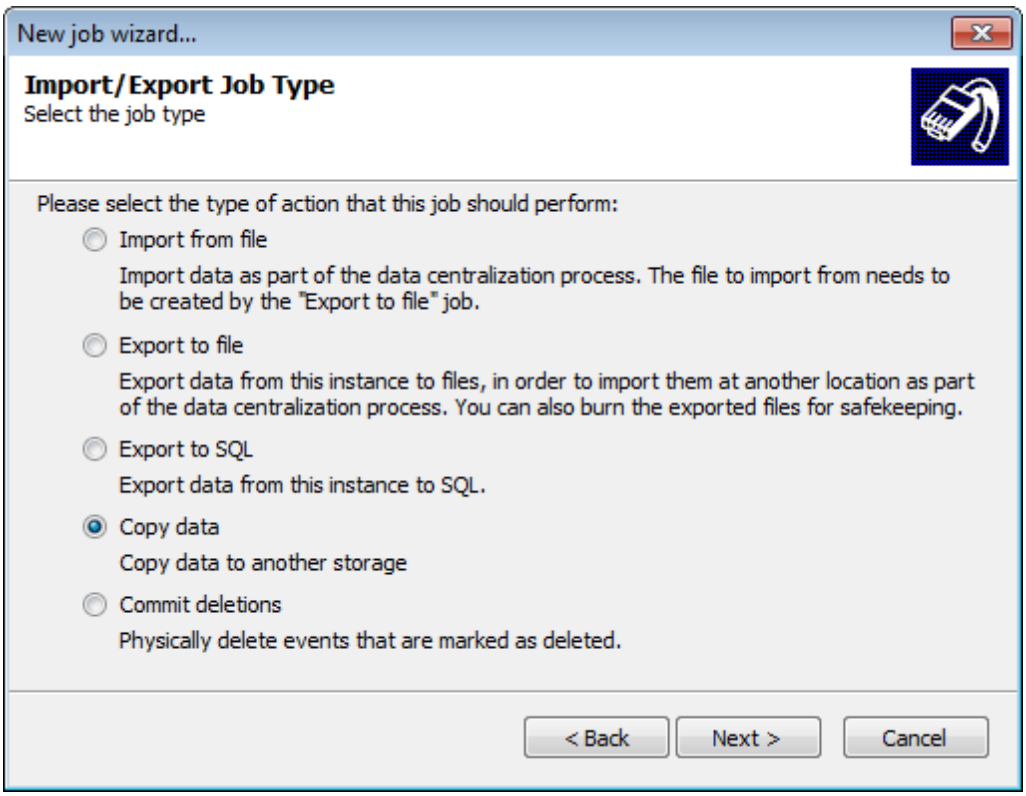
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

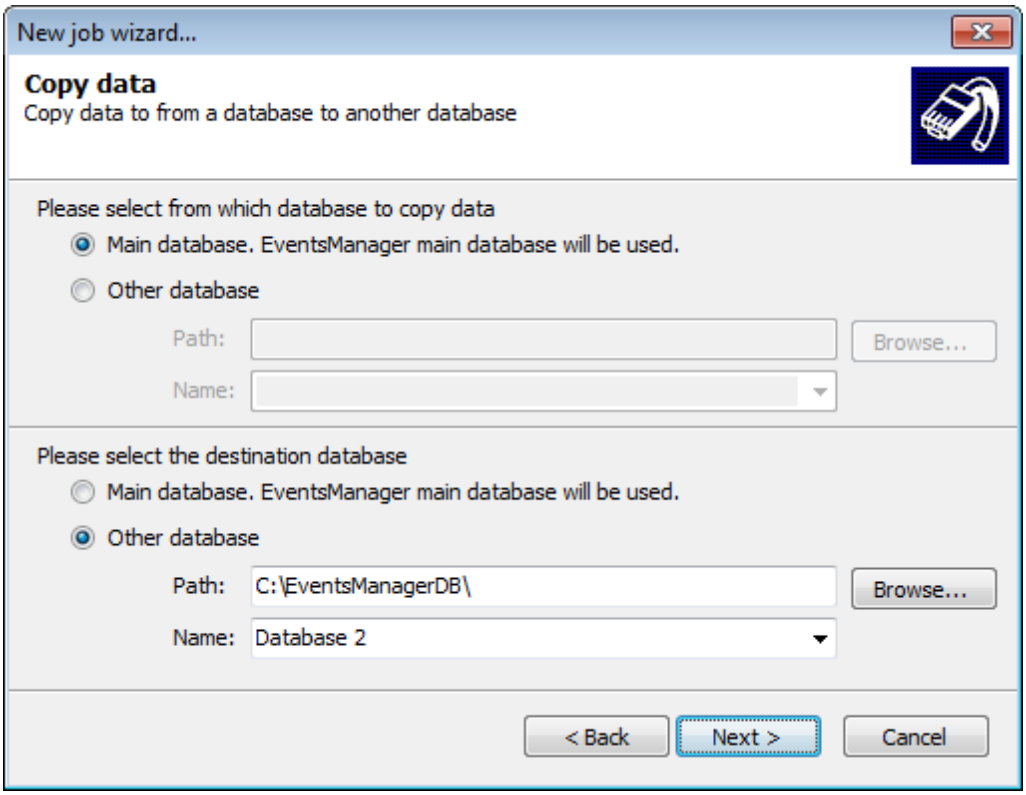
Captura de pantalla 224: Crear tareas de importación/exportación

4. Seleccione **Import/Export Job** y haga clic en **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

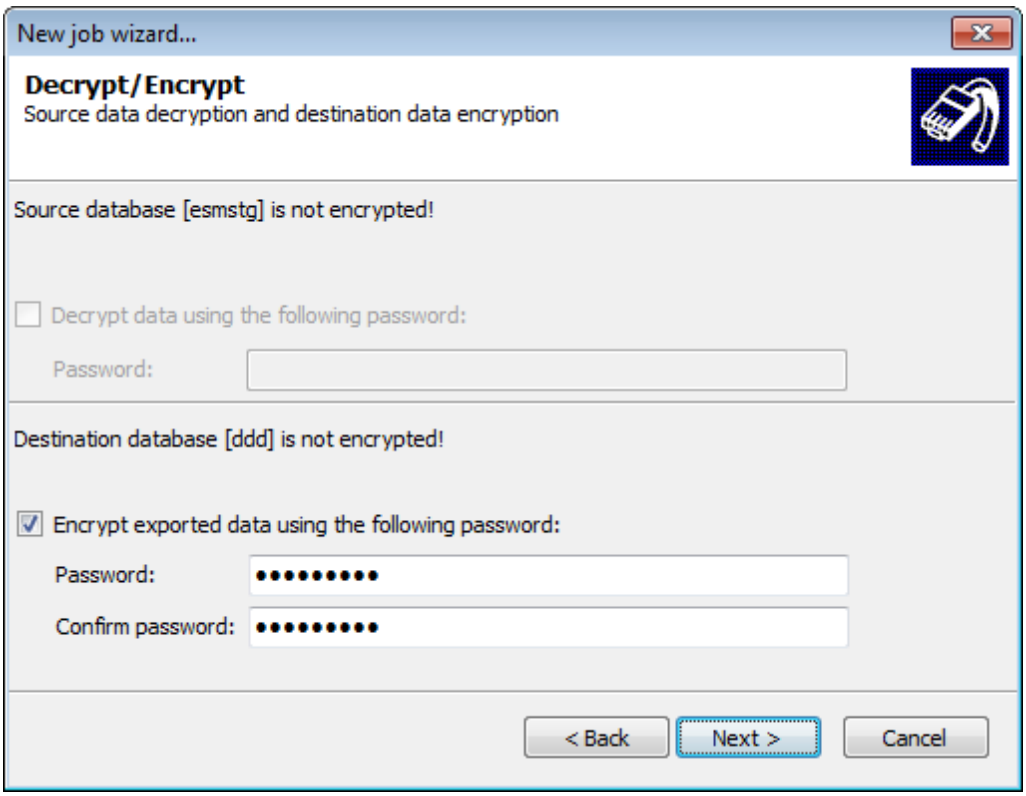
Captura de pantalla 225: Seleccionar tarea de copia de datos

5. Seleccione **Copy data** y haga clic en **Next**.



Captura de pantalla 226: Especificar bases de datos de origen y destino

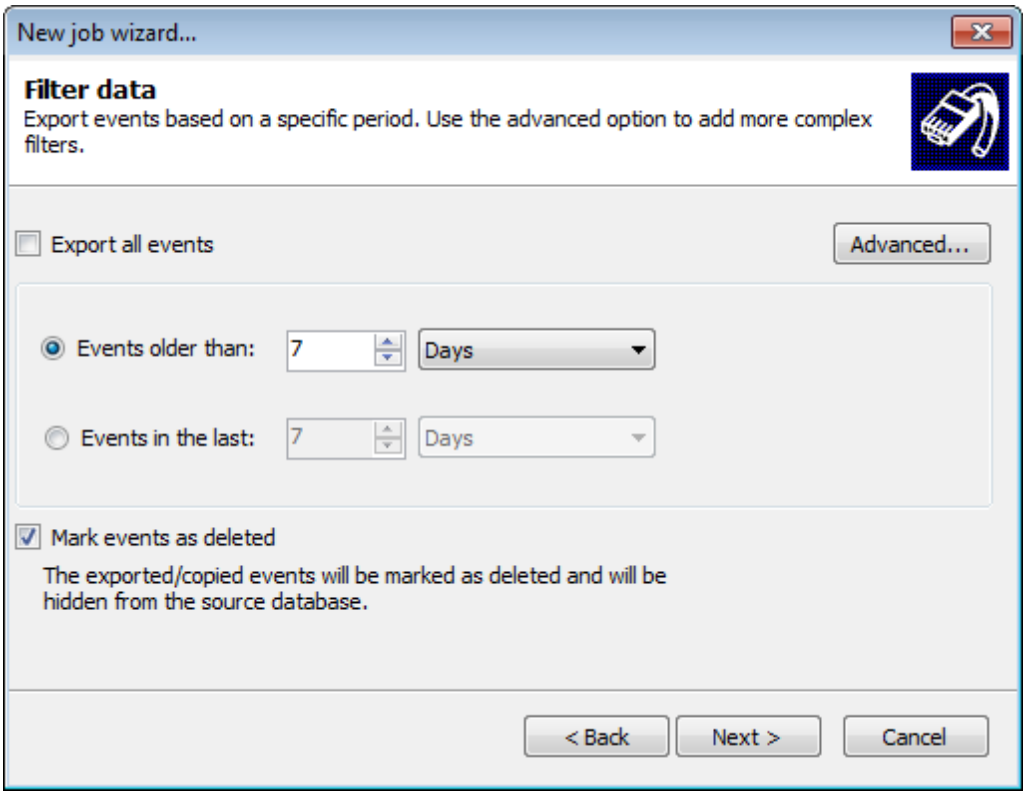
6. Seleccione las bases de datos de origen y destino. Haga clic en **Siguiente**.



Captura de pantalla 227: Descifrar y cifrar las bases de datos de origen y destino

7. Si la base de datos de origen está cifrada, seleccione **Decrypt data using the following password** y especifique la contraseña utilizada para cifrar la base de datos.

8. Si desea cifrar los datos de origen, seleccione **Encrypt exported data using the following password**. Especifique la contraseña de cifrado y haga clic en **Next**.


New job wizard...
Filter data
Export events based on a specific period. Use the advanced option to add more complex filters.
Export all events
Advanced...
Events older than:
7
Days
Events in the last:
7
Days
Mark events as deleted
The exported/copied events will be marked as deleted and will be hidden from the source database.
< Back
Next >
Cancel

Captura de pantalla 228: Filtrar datos exportados

9. Configure las siguientes opciones de filtro y haga clic en **Next**:

Tabla 90: Filtrar datos exportados

Opción	Descripción
Export all events	Exporta todos los eventos de la base de datos.
Events older than	Solamente se exportan los eventos anteriores al número especificado de días/semanas/meses.
Events in the last	Solamente se exportan los eventos que ocurrieron en el último número especificado de días/semanas/meses.
Mark events as deleted	Permite ocultar los eventos de la base de datos de origen después de exportarlos. Para eliminar completamente estos eventos de la base de datos, debe ejecutar una tarea de confirmar eliminaciones. Para obtener más información, consulte Confirmar eliminaciones.
Advanced...	Haga clic en Advanced... para iniciar el cuadro de diálogo Advanced Filtering. Le permite configurar parámetros de filtro granulares para exportar únicamente eventos específicos. Para obtener más información, consulte Diseñar restricciones de consulta.

10. Seleccione cuándo se ejecuta la tarea y haga clic en **Finish**:

Tabla 91: Crear tareas de mantenimiento - Opciones de programación

Opciones	Descripción
Schedule job	La tarea se guardará y se ejecutará de acuerdo con la programación de operaciones de la base de datos.
Run the job now	La tarea se ejecuta inmediatamente. Las tareas no programadas solamente se ejecutan una vez y no pueden ser reutilizadas.

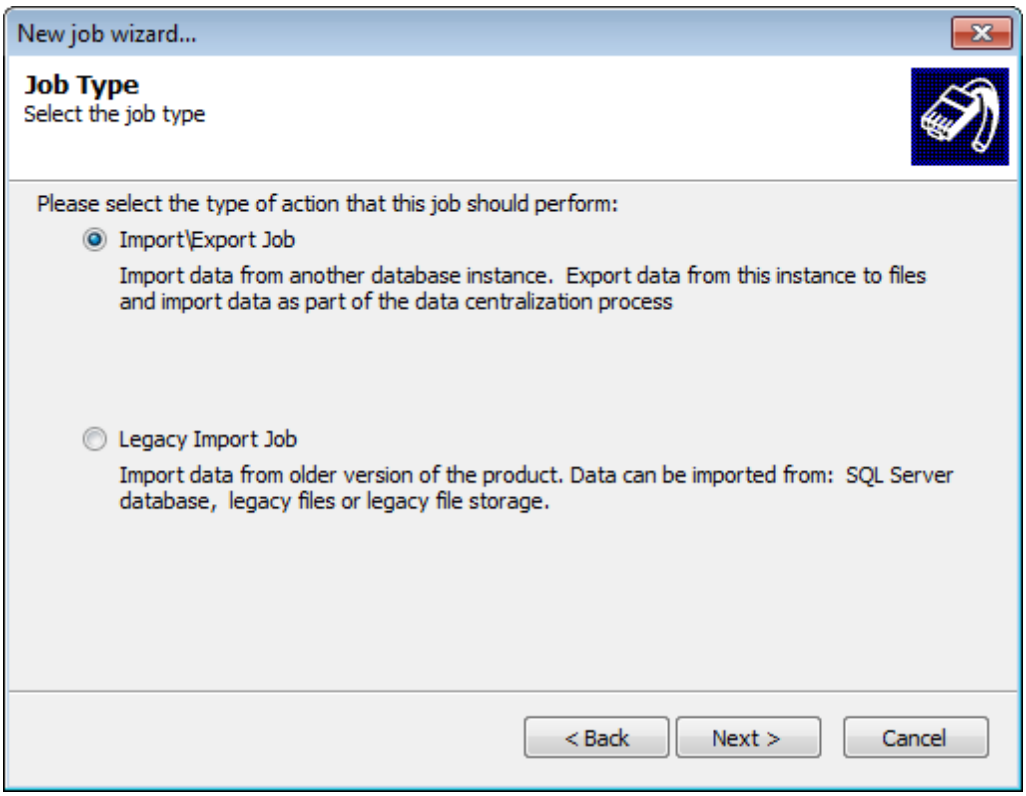
14.2.5 Confirmar eliminaciones

Para crear tareas de confirmación de eliminación:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

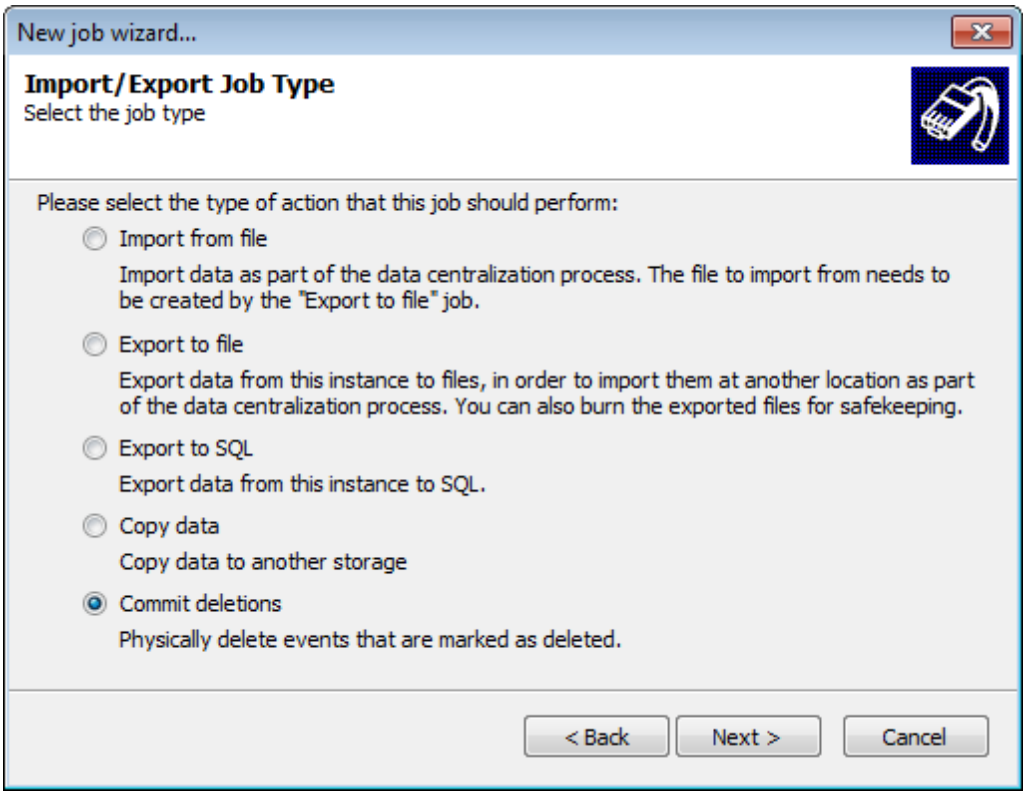
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

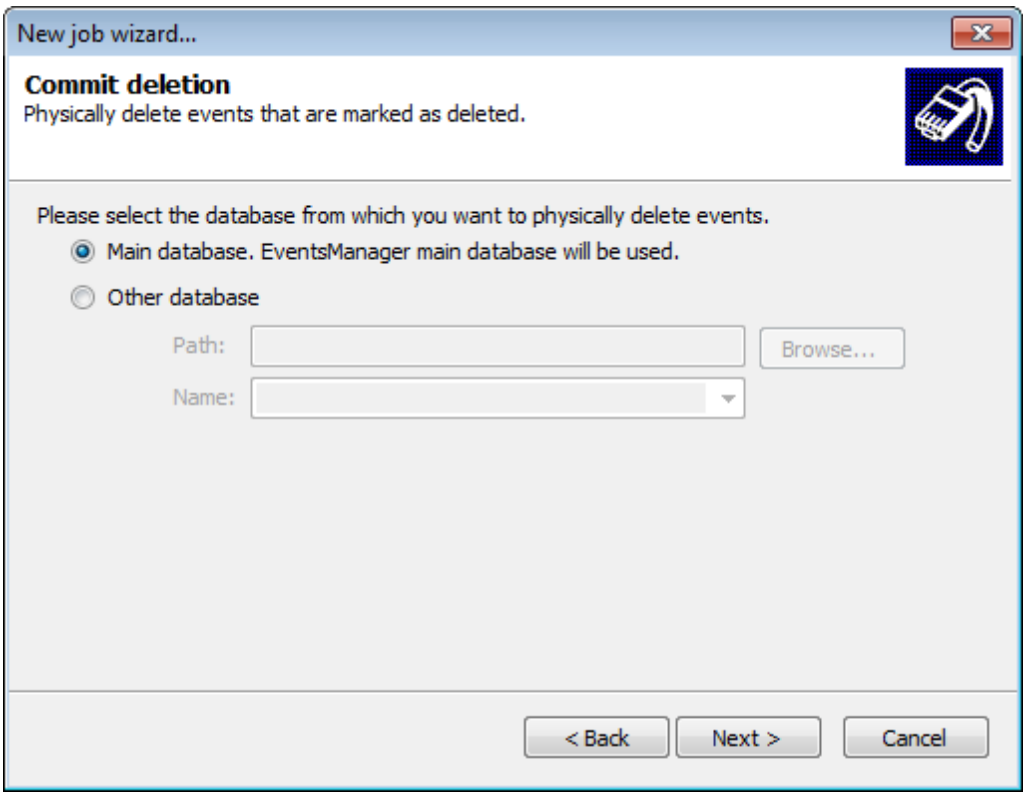
Captura de pantalla 229: Crear tareas de importación/exportación

4. Seleccione **Import/Export Job** y haga clic en **Next**.


New job wizard...
Import/Export Job Type
Select the job type
Please select the type of action that this job should perform:
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Export to SQL
Export data from this instance to SQL.
Copy data
Copy data to another storage
Commit deletions
Physically delete events that are marked as deleted.
< Back
Next >
Cancel

Captura de pantalla 230: Crear tareas de confirmación de eliminación

5. Seleccione **Commit deletions** y haga clic en **Next**.



Captura de pantalla 231: Seleccionar la base de datos de la que desea eliminar los registros.

6. Seleccione la base de datos de la que desea eliminar los registros. Haga clic en **Siguiente**.

7. Seleccione cuándo se ejecuta la tarea y haga clic en **Finish**:

Tabla 92: Crear tareas de mantenimiento - Opciones de programación

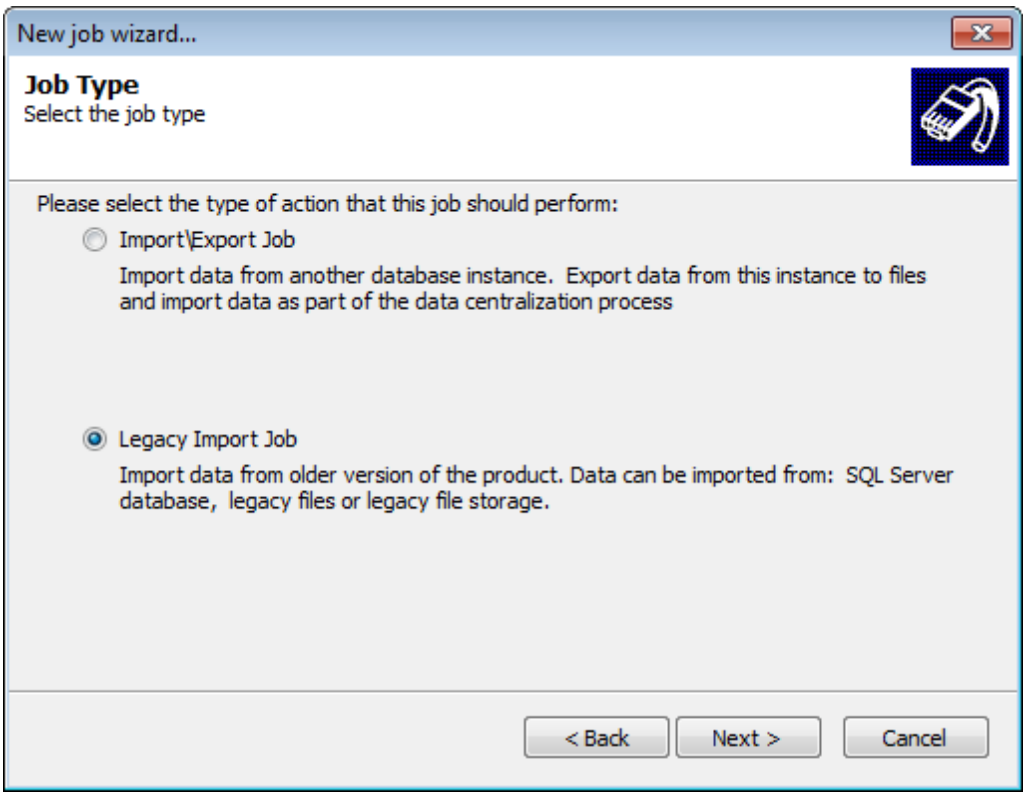
Opciones	Descripción
Schedule job	La tarea se guardará y se ejecutará de acuerdo con la programación de operaciones de la base de datos.
Run the job now	La tarea se ejecuta inmediatamente. Las tareas no programadas solamente se ejecutan una vez y no pueden ser reutilizadas.

14.2.6 Importar desde la base de datos de SQL Server®

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

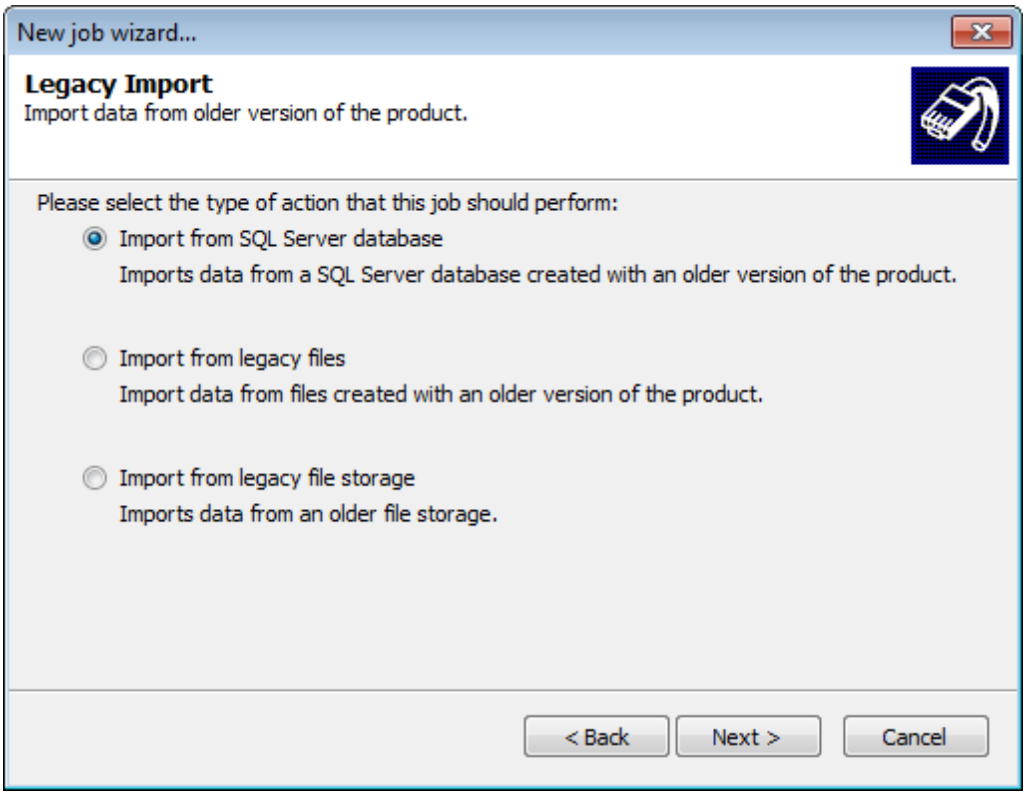
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

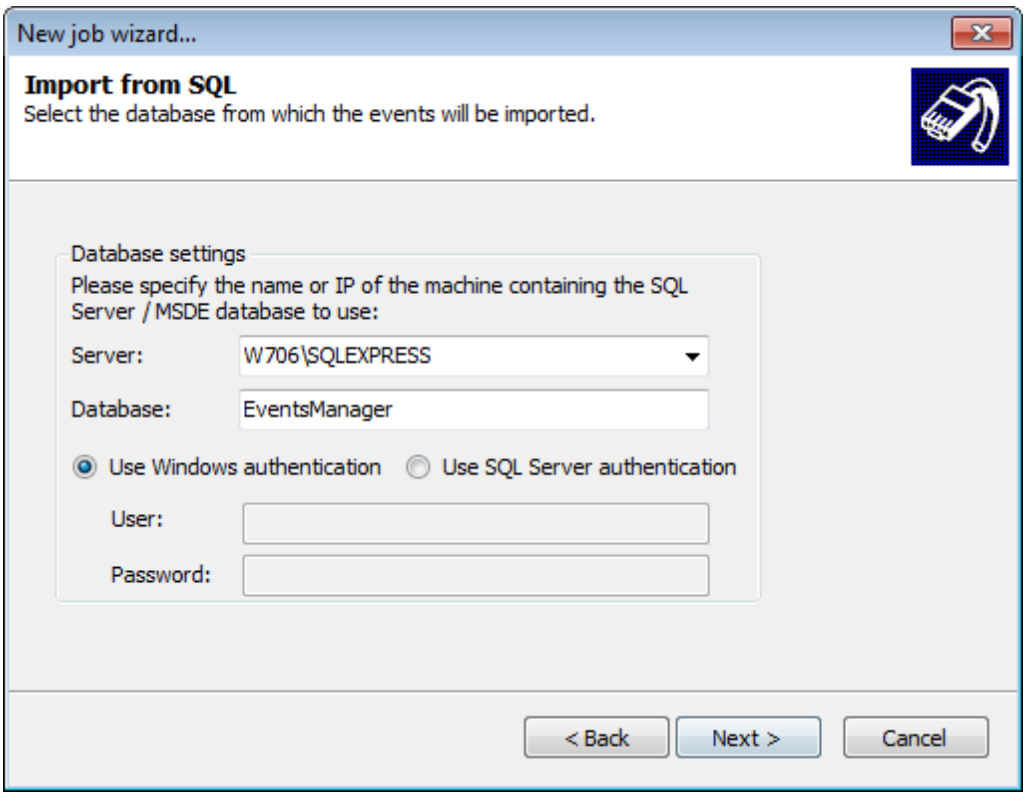
Captura de pantalla 232: Crear tareas de importación/exportación

4. Seleccione **Legacy Import Job** y haga clic en **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

Captura de pantalla 233: Seleccionar Import from SQL Server Database

5. Seleccione **Import from SQL Server® database** y haga clic en **Next**.

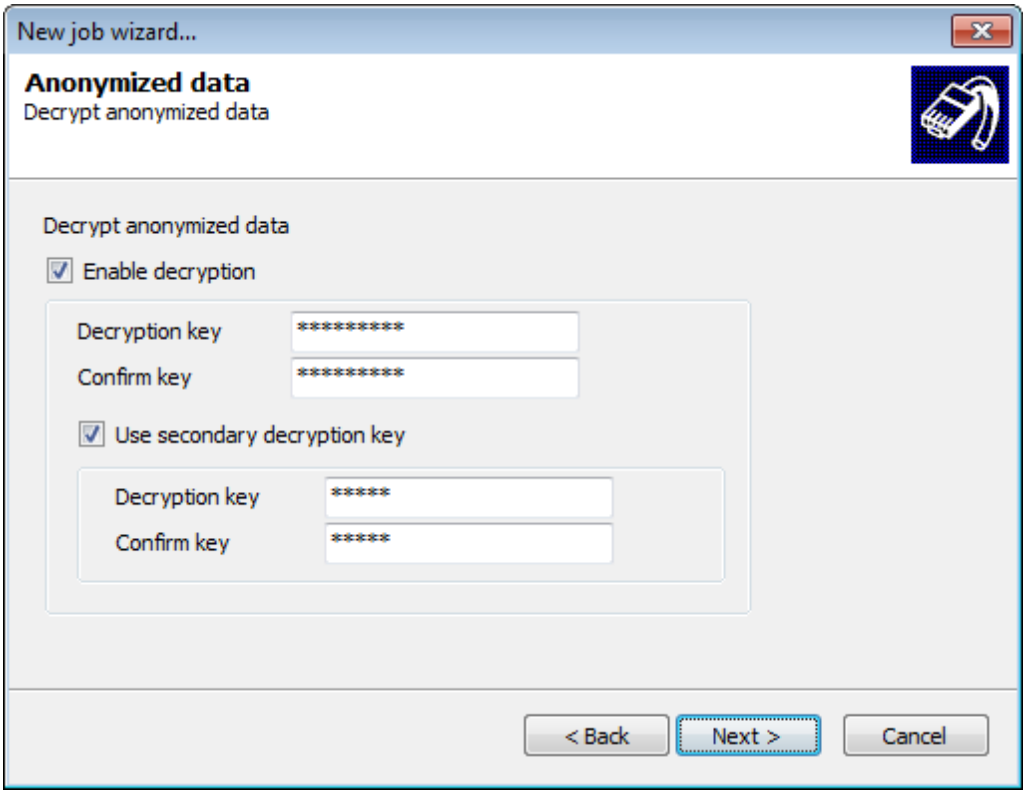


Captura de pantalla 234: Especificar dirección y datos de acceso a SQL Server

6. Configure las siguientes opciones de servidor y haga clic en **Next**:

Tabla 93: Exportar a SQL: Opciones del servidor

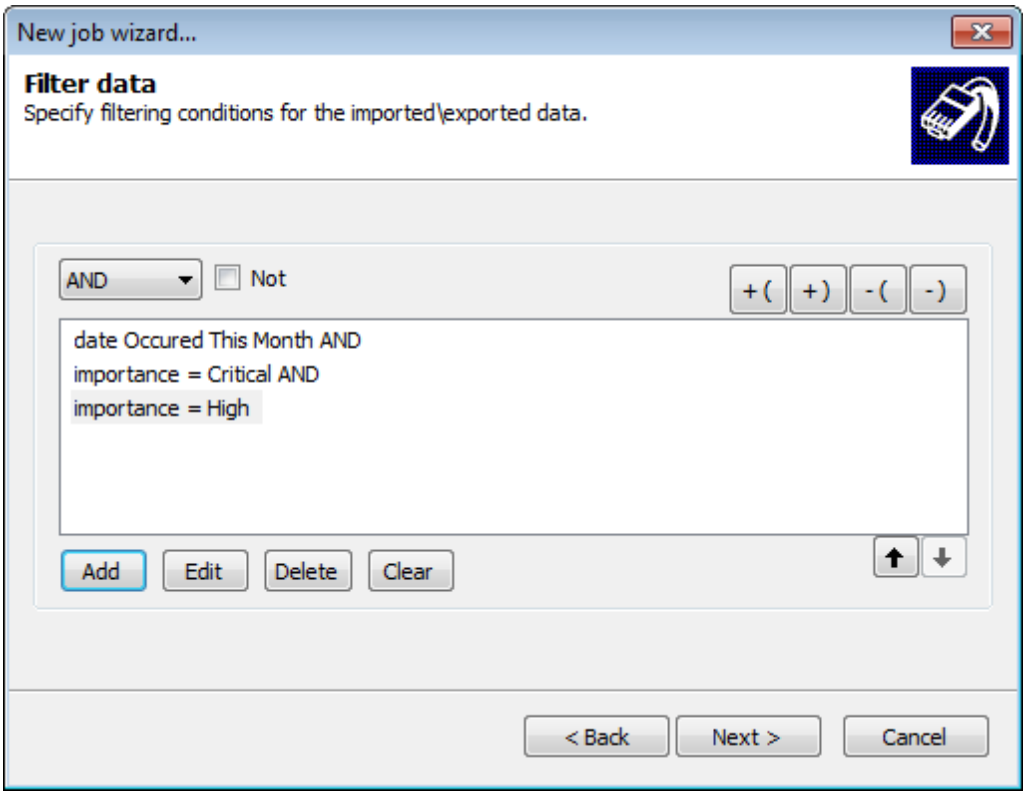
Opción	Descripción
Server	Escriba el nombre de la máquina que está ejecutando SQL Server.
Base de datos	Escriba el nombre de la base de datos de origen.
Use Windows authentication	Se usan las mismas credenciales de inicio de sesión que se usan para iniciar sesión en Windows®. SQL Server® debe admitir este tipo de modo de autenticación para poder conectarse y copiar información desde el servidor.
Use SQL Server authentication	Se usan las credenciales de inicio de sesión configuradas en su SQL Server®. Escriba el nombre de usuario en el campo **User** y la contraseña en el campo **Password**.



Captura de pantalla 235: Descifrar bases de datos anonimizadas

7. (Opcional) Si la base de datos de SQL Server® está anonimizada, seleccione **Enable decryption** y especifique la contraseña que se usó para anonimizar la base de datos.

8. (Opcional) Si la base de datos de SQL Server está anonimizada con dos contraseñas, seleccione **Use secondary decryption key** y especifique la clave de seguridad secundaria que se usó para anonimizar la base de datos. Haga clic en **Siguiente**.

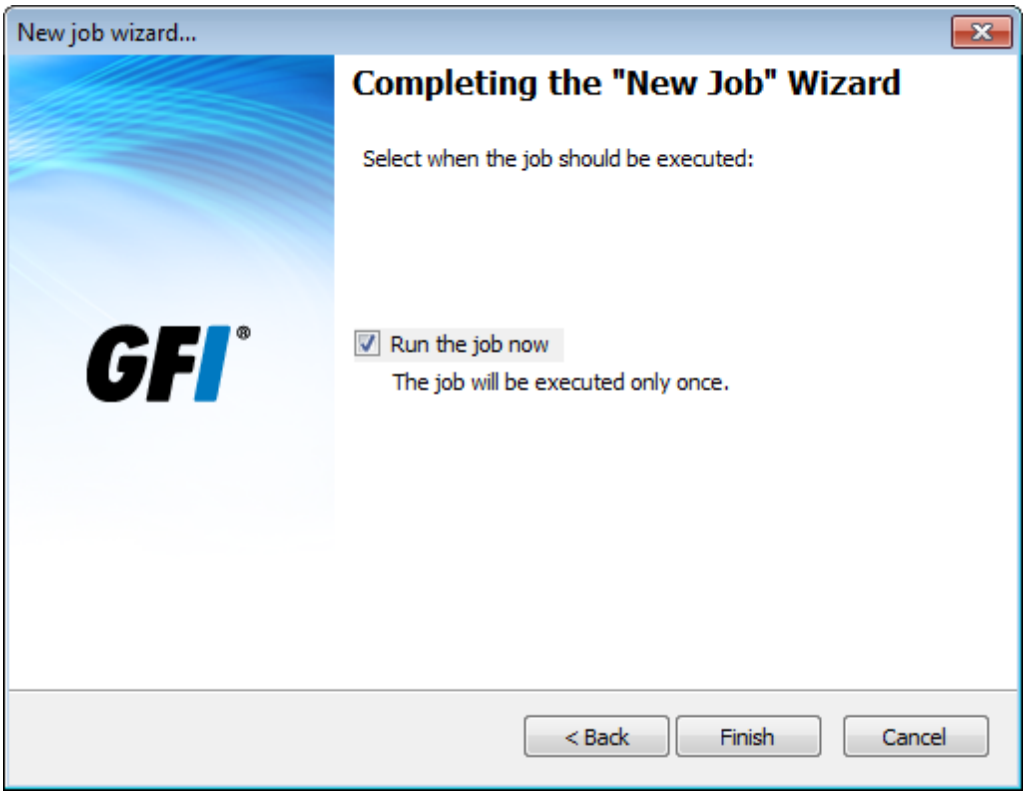


Captura de pantalla 236: Agregar condiciones de filtrado para filtrar datos no deseados

9. Agregue parámetros de filtrado avanzado para importar solamente datos específicos. Deje en blanco esta opción para importar todos los registros de eventos.

Nota

Para obtener más información, consulte Diseñar restricciones de consultas.



Captura de pantalla 237: Especificar cuándo se ejecuta la tarea de mantenimiento

Seleccione **Run the job now** y haga clic en **Finish**.

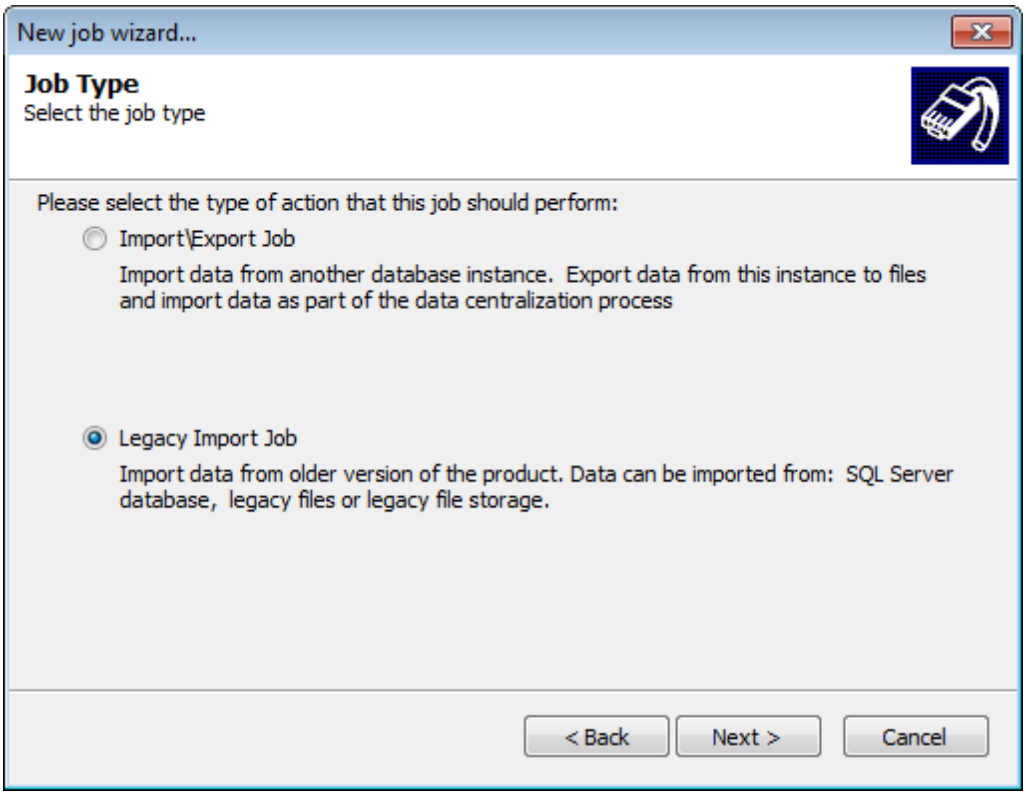
14.2.7 Importar desde archivos heredados

Para importar desde tareas de archivos heredados:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

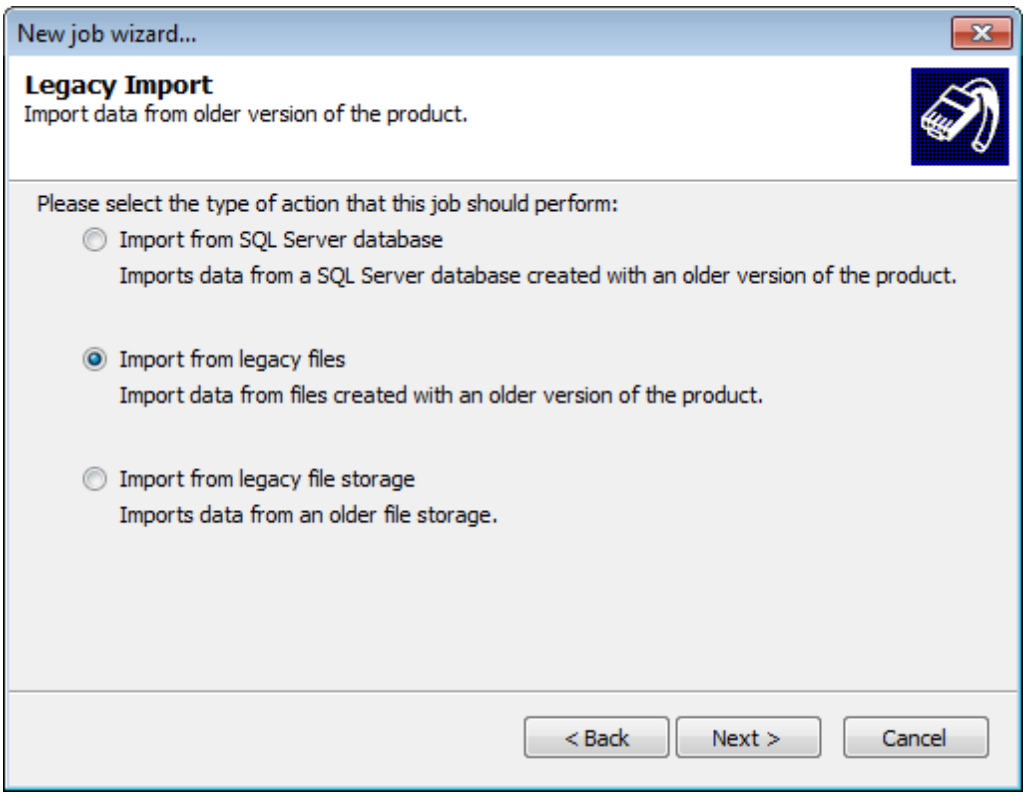
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

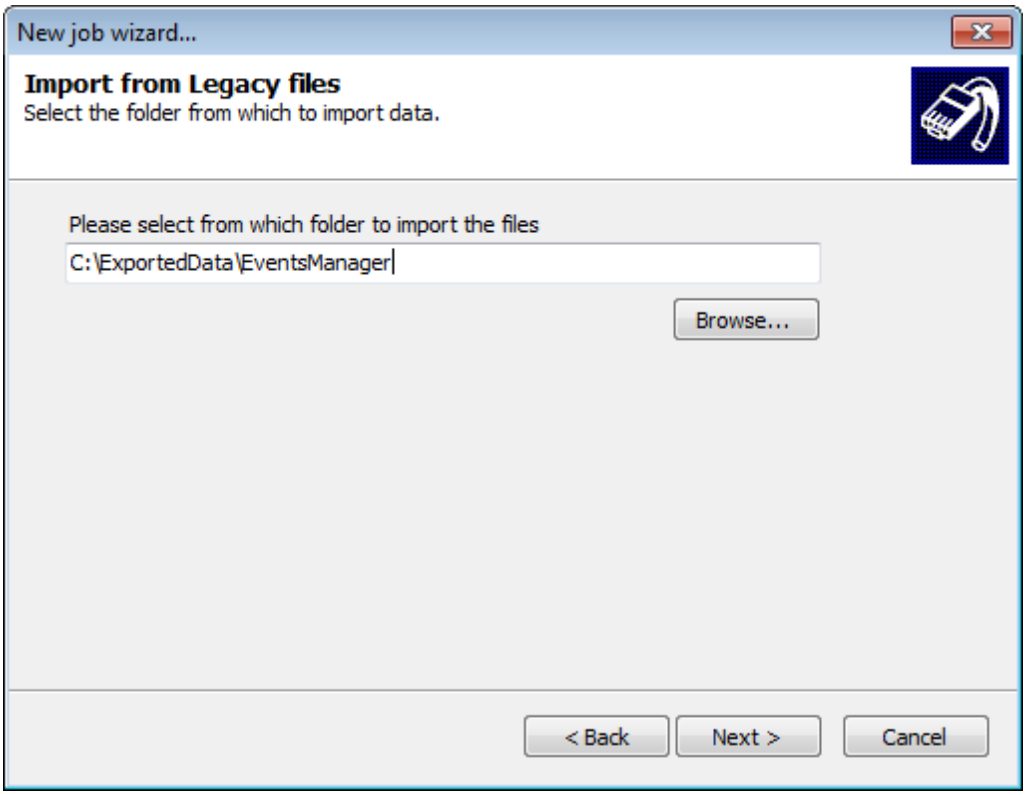
Captura de pantalla 238: Crear tareas de importación/exportación

4. Seleccione **Legacy Import Job** y haga clic en **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

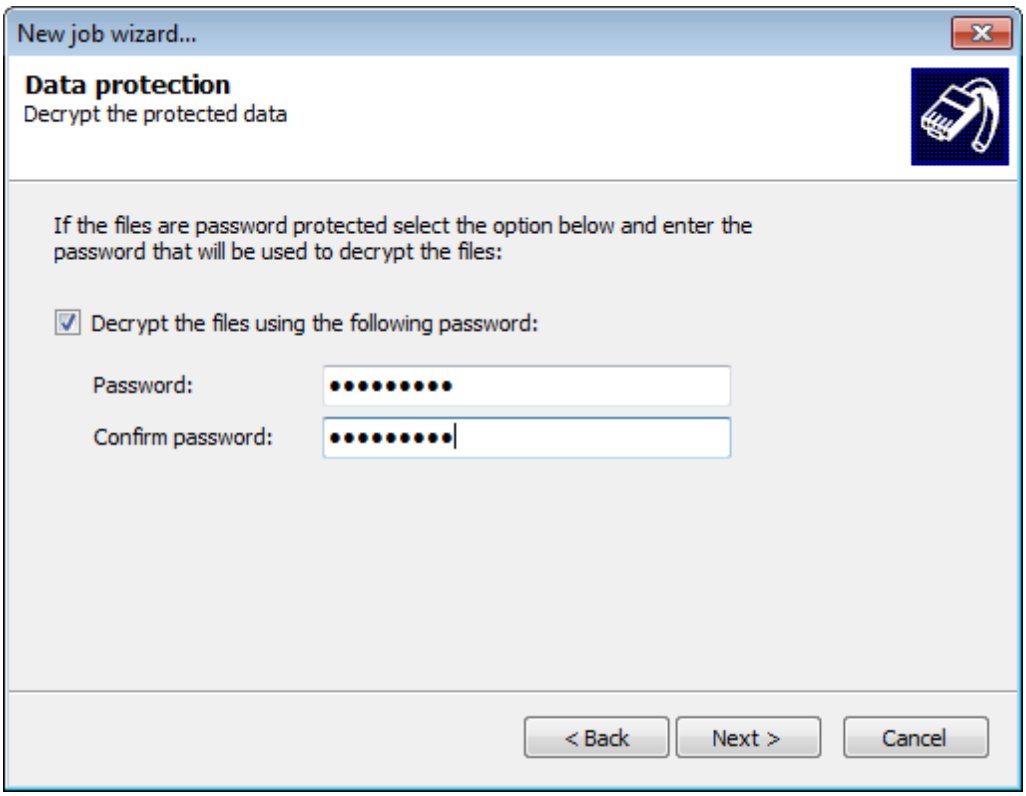
Captura de pantalla 239: Importar desde archivos heredados

5. Seleccione **Import from legacy files** y haga clic en **Next**.



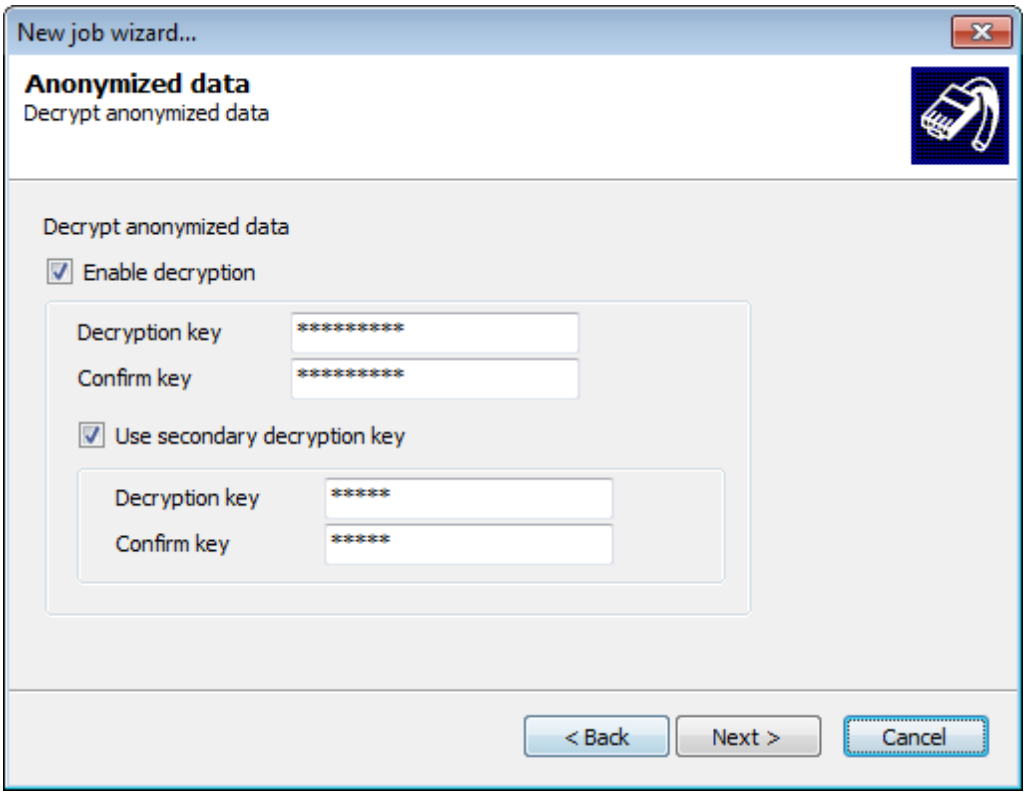
Captura de pantalla 240: Especificar ubicación del archivo de importación

6. Especifique la ruta de acceso al archivo de configuración que contiene los datos que desea importar. Opcionalmente, haga clic en **Browse** para buscar la ubicación. Haga clic en **Siguiente**.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Captura de pantalla 241: Descifrar información en el archivo de importación

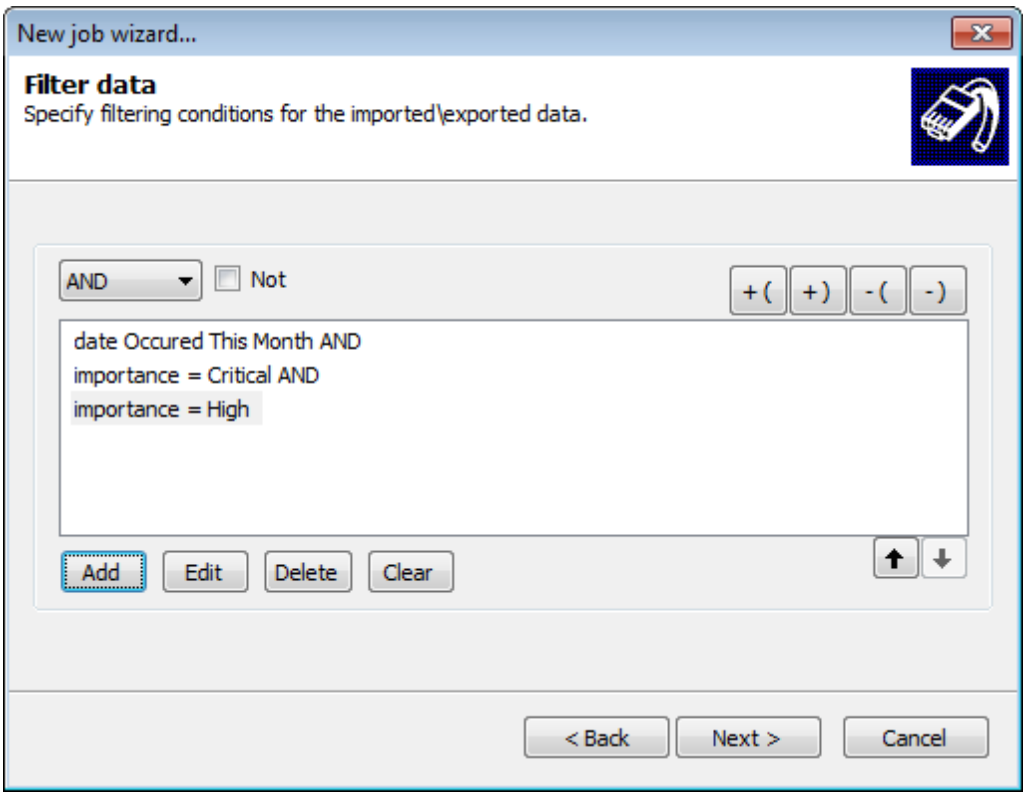
7. (Opcional) Si se cifró el archivo, seleccione **Decrypt the files using the following password** y especifique la contraseña que se usó para cifrar el archivo. Haga clic en **Siguiente**.



Captura de pantalla 242: Quitar anonimización

8. (Opcional) Si el archivo está anonimizado, seleccione **Enable decryption** y especifique la contraseña que se usó para anonimizar los datos.

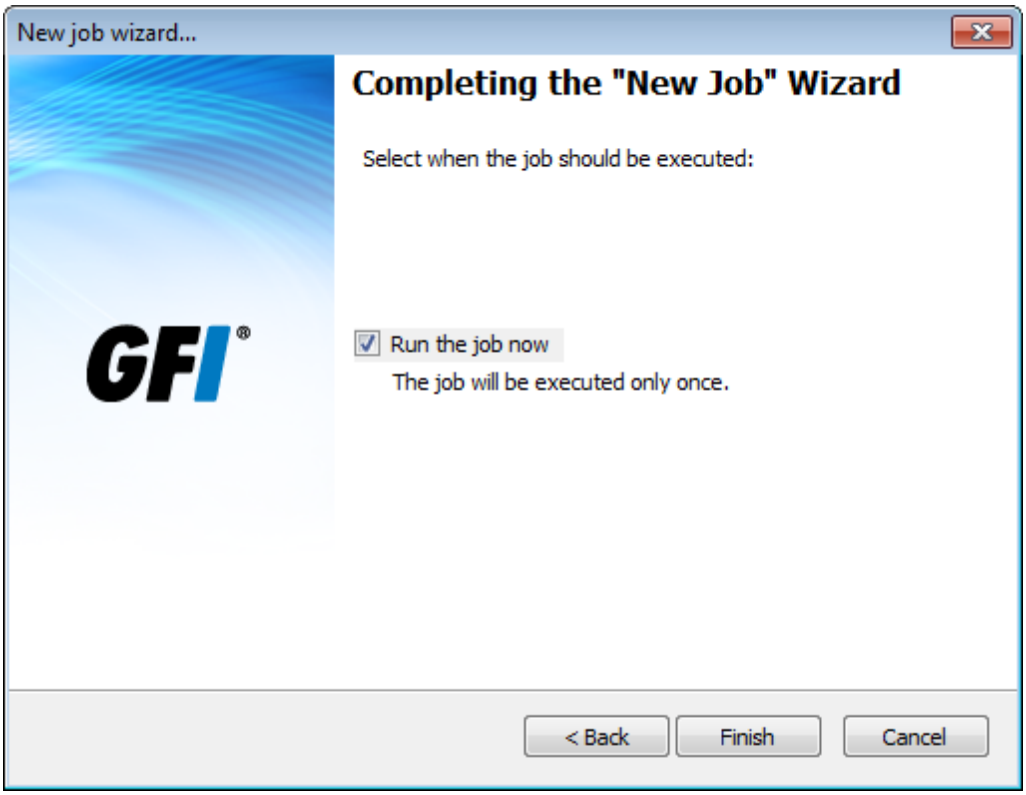
9. (Opcional) Si el archivo se anonimizó con dos contraseñas, seleccione **Use secondary decryption key** y especifique la segunda clave que se usó para anonimizar los datos dentro del archivo. Haga clic en **Siguiente**.



Captura de pantalla 243: Filtrar eventos no deseados por medio de condiciones de filtrado

10. Agregue parámetros de filtrado avanzado para importar solamente datos específicos. Deje en blanco esta opción para importar todos los registros de eventos.

> **Nota**
>
> Para obtener más información, consulte Diseñar restricciones de consultas.



Captura de pantalla 244: Especificar cuándo se ejecuta la tarea de mantenimiento

Seleccione **Run the job now** y haga clic en **Finish**.

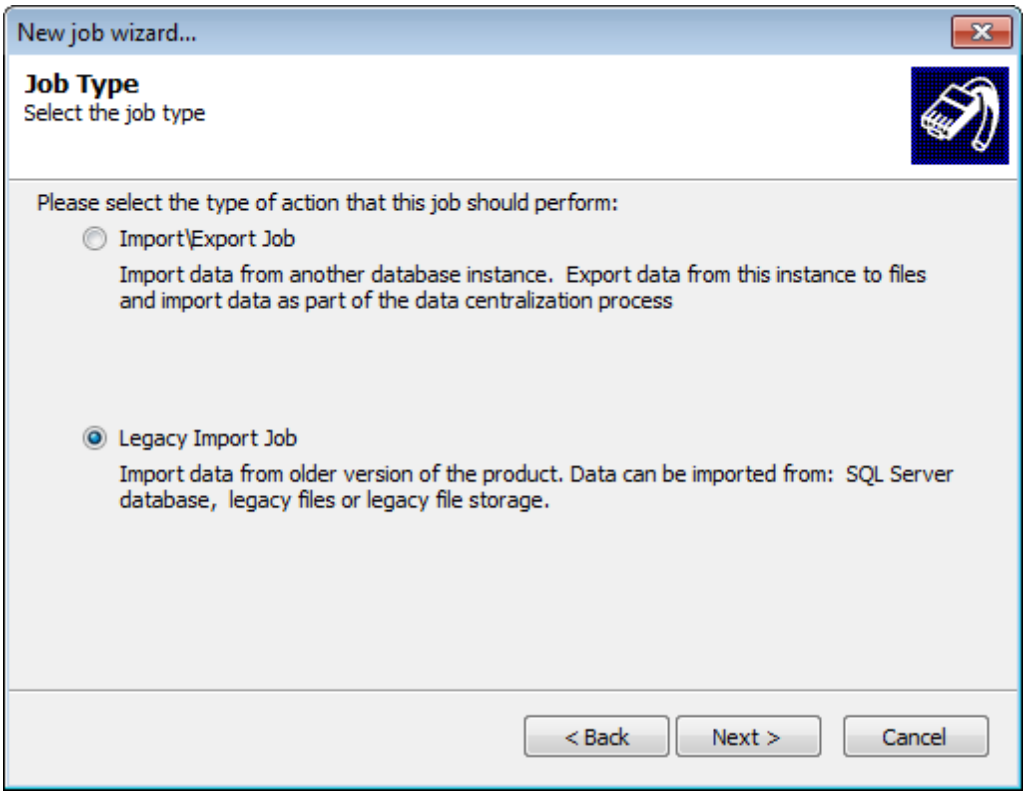
14.2.8 Importar desde almacenamiento de archivos heredados

Para importar desde tareas de archivos heredados:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

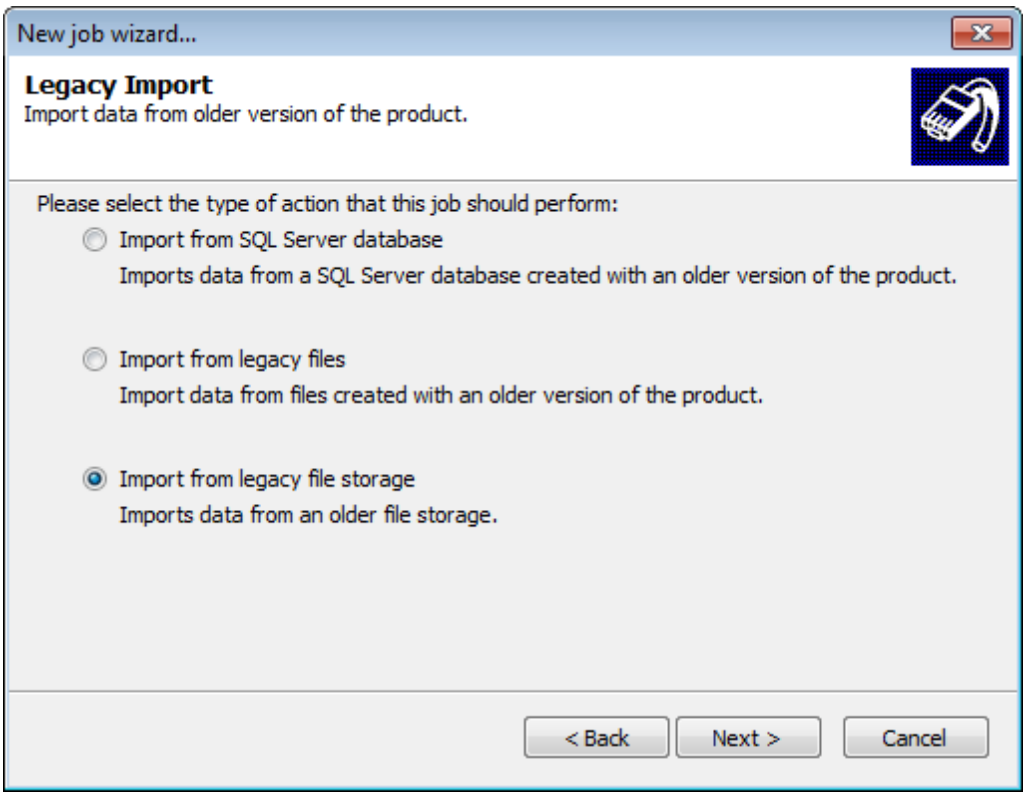
2. En **Configurations**, haga clic con el botón secundario en el nodo **Database Operations** y seleccione **Create new job…**.

3. Haga clic en **Next** en la pantalla de bienvenida del asistente.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Import\Export Job
Import data from another database instance. Export data from this instance to files and import data as part of the data centralization process
Legacy Import Job
Import data from older version of the product. Data can be imported from: SQL Server database, legacy files or legacy file storage.
< Back
Next >
Cancel

Captura de pantalla 245: Crear tareas de importación/exportación

4. Seleccione **Legacy Import Job** y haga clic en **Next**.


New job wizard...
Legacy Import
Import data from older version of the product.
Please select the type of action that this job should perform:
Import from SQL Server database
Imports data from a SQL Server database created with an older version of the product.
Import from legacy files
Import data from files created with an older version of the product.
Import from legacy file storage
Imports data from an older file storage.
< Back
Next >
Cancel

Captura de pantalla 246: Importar datos desde almacenamiento de archivos heredados

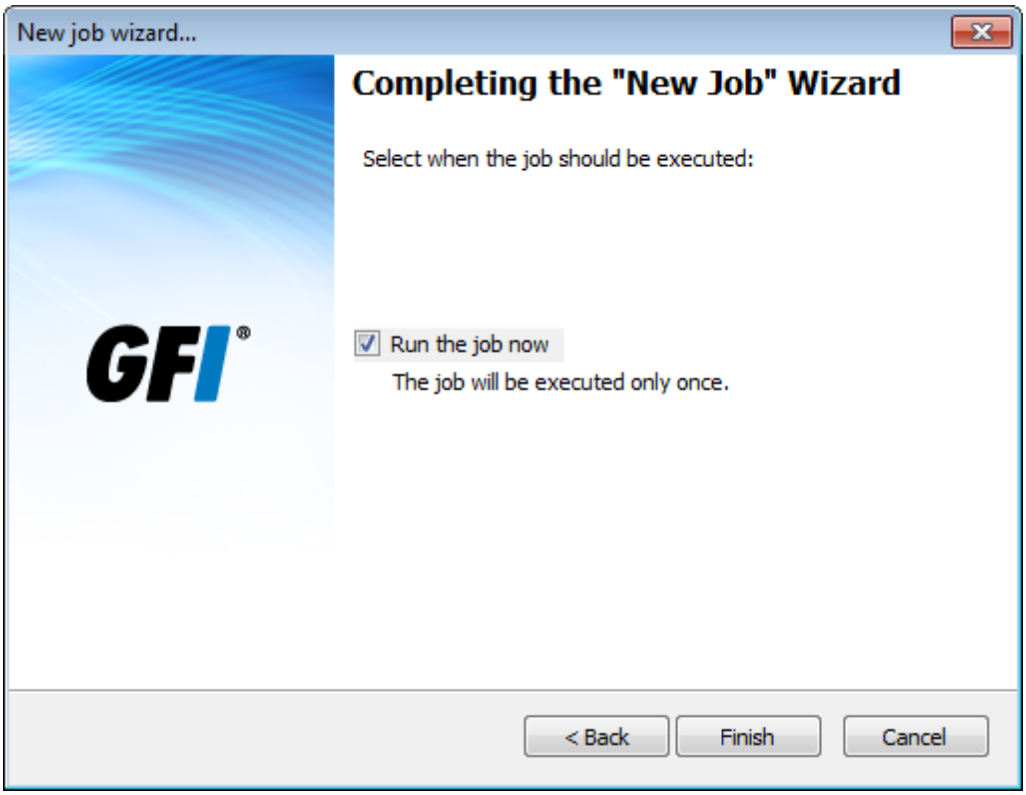
5. Seleccione **Import from legacy file storage** y haga clic en **Next**.

6. Especifique la ruta donde se ubica el archivo de importación. O bien, haga clic en **Browse** y busque la ubicación.

7. (Opcional) Si los datos están anonimizados, seleccione **Enable decryption** y especifique la contraseña que se usó para cifrar los datos.

8. (Opcional) Si los datos están cifrados con dos contraseñas, seleccione **Use secondary decryption** y escriba la contraseña secundaria. Haga clic en **Siguiente**.

9. (Opcional) Especifique las condiciones de filtrado para filtrar los datos no deseados. Déjelo en blanco para exportar todos los datos en la base de datos. Para obtener más información, consulte Definir restricciones. Haga clic en **Siguiente**.



Captura de pantalla 247: Especificar cuándo se ejecuta la tarea de mantenimiento

Seleccione **Run the job now** y haga clic en **Finish**.

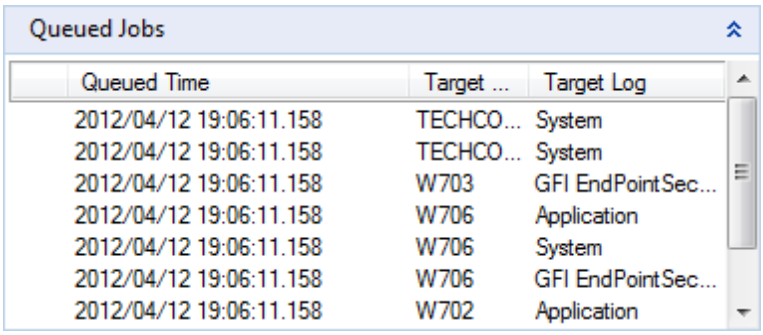
14.3 Editar tareas de mantenimiento

Esta sección contiene información acerca de:

- Ver tareas de mantenimiento programadas
- Editar propiedades de la tarea de mantenimiento
- Cambiar prioridad de las tareas de mantenimiento
- Eliminar tarea de mantenimiento

14.3.1 Ver tareas de mantenimiento programadas

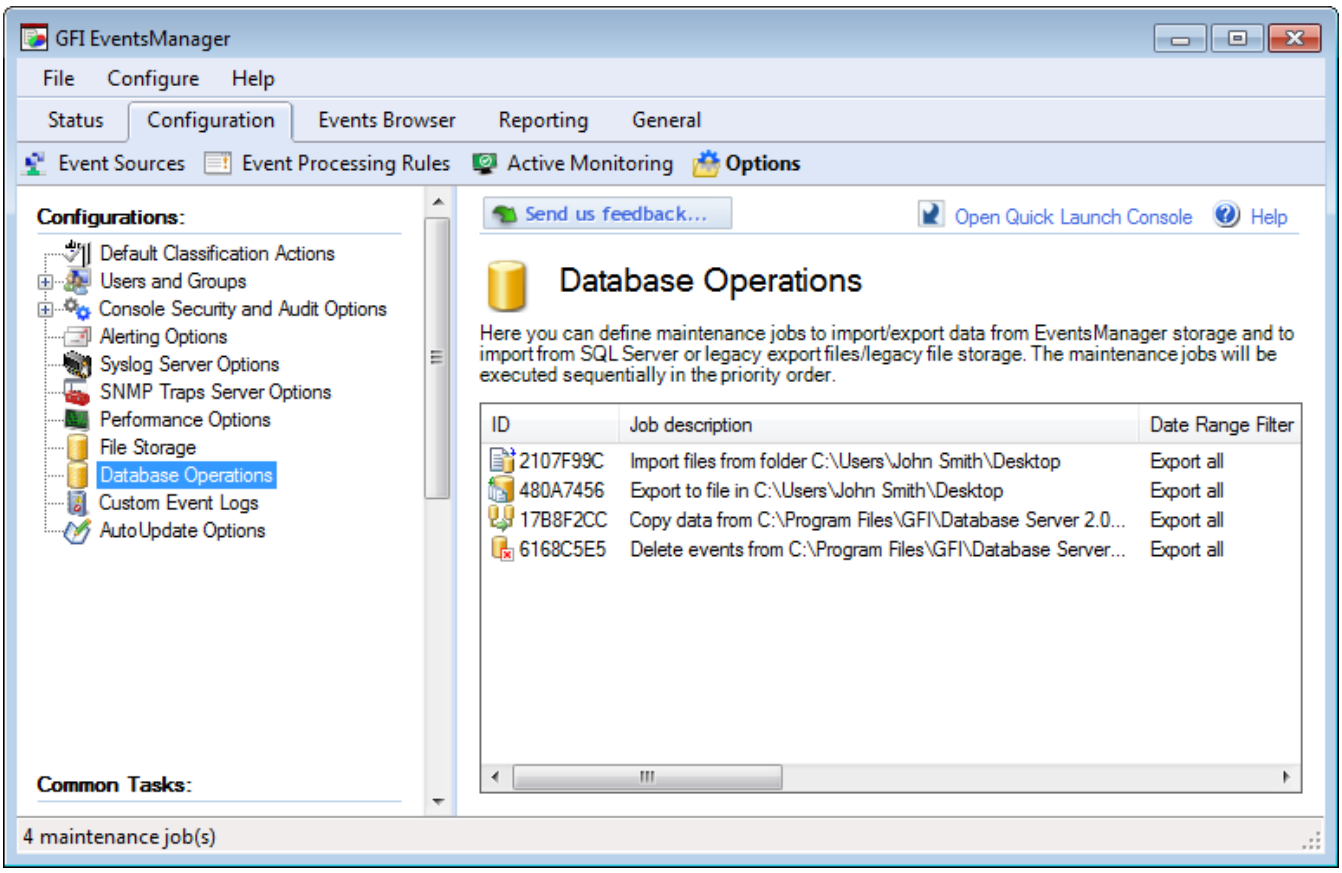
Para ver el progreso de las tareas de mantenimiento programadas:



Captura de pantalla 248: Actividad de las tareas de mantenimiento

Haga clic en la ficha **Status > Job Activity**. El estado de todas las tareas de mantenimiento se mostrará en la sección **Queued Jobs**.

Para ver las tareas de mantenimiento creadas:


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Event Sources Event Processing Rules Active Monitoring Options
Configurations:
Default Classification Actions
Users and Groups
Console Security and Audit Options
Alerting Options
Syslog Server Options
SNMP Traps Server Options
Performance Options
File Storage
Database Operations
Custom Event Logs
AutoUpdate Options
Common Tasks:
Send us feedback...
Open Quick Launch Console
Help
Database Operations
Here you can define maintenance jobs to import/export data from EventsManager storage and to import from SQL Server or legacy export files/legacy file storage. The maintenance jobs will be executed sequentially in the priority order.
ID
Job description
Date Range Filter
2107F99C Import files from folder C:\Users\John Smith\Desktop Export all
480A7456 Export to file in C:\Users\John Smith\Desktop Export all
17B8F2CC Copy data from C:\Program Files\GFI\Database Server 2.0... Export all
6168C5E5 Delete events from C:\Program Files\GFI\Database Server... Export all
4 maintenance job(s)

Captura de pantalla 249: Ver las tareas de mantenimiento programadas

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

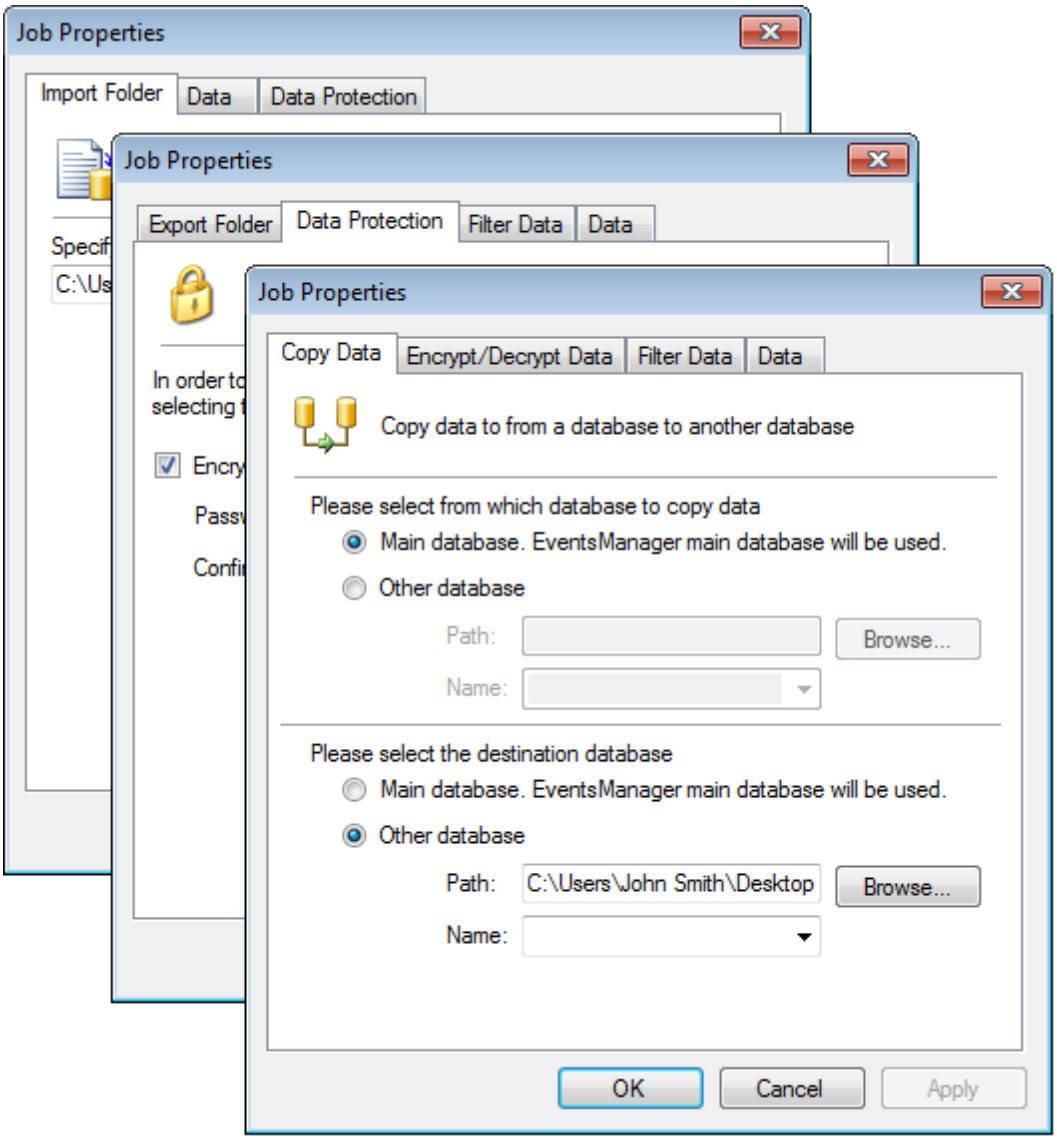
2. En **Configurations**, seleccione el nodo **Database Operations**. Las tareas de mantenimiento programadas se muestran en el panel derecho.

14.3.2 Editar propiedades de las tareas de mantenimiento

Para editar las propiedades de las tareas de mantenimiento:

1. En la ficha **Configuration > Options > Configurations**, haga clic en **Database Operations**.

2. En el panel derecho, haga clic con el botón secundario en una tarea de mantenimiento y seleccione **Properties**.



Captura de pantalla 250: Cuadro de diálogo Maintenance job properties

3. En el cuadro de diálogo Maintenance job properties, puede modificar los parámetros que configuró al crear la tarea, como:

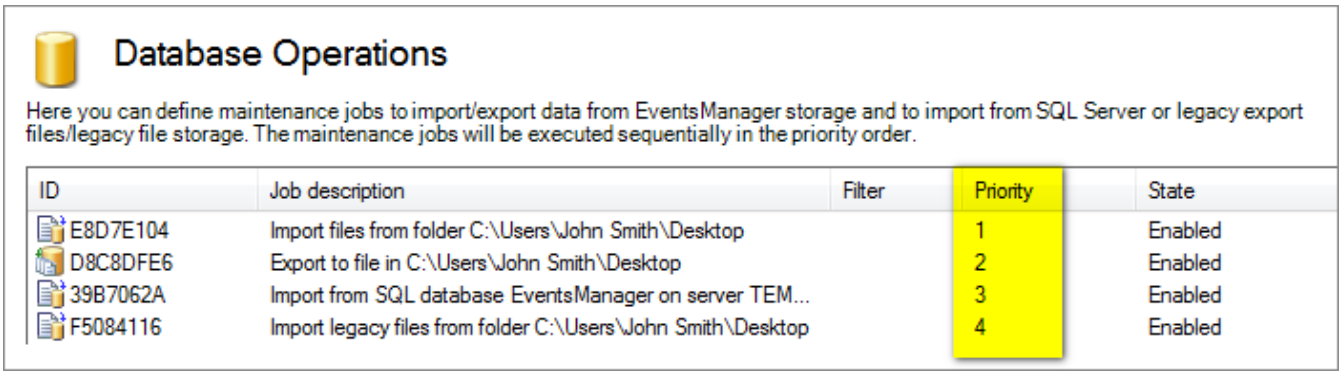
- Contraseñas de cifrado/descifrado
- Nombres y direcciones de bases de datos
- Rutas de acceso de origen/destino
- Detalles generales de las tareas

4. Haga clic en **Apply** y **OK**.

Nota

Para obtener más información, consulte Crear tareas de mantenimiento.

14.3.3 Cambiar prioridad de las tareas de mantenimiento



Captura de pantalla 251: Prioridades de las tareas de mantenimiento

De forma predeterminada, las tareas de mantenimiento se llevan a cabo según la secuencia con la que se crean las tareas (primero en entrar, primero en salir). Por lo tanto, la secuencia en la que se ejecutan las tareas determina la prioridad de las tareas de mantenimiento.

Para aumentar o disminuir la prioridad de una tarea de mantenimiento:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

2. En **Configurations**, seleccione **Database Operations**.

3. En el panel derecho, haga clic con el botón secundario en la tarea de mantenimiento y seleccione **Increase Priority** o **Decrease Priority** según corresponda.

14.3.4 Eliminar una tarea de mantenimiento

Para eliminar tareas de mantenimiento:

1. Haga clic en la ficha **Configuration** y seleccione **Options**.

2. En **Configurations**, seleccione **Database Operations**.

3. En el panel derecho, haga clic con el botón secundario en la tarea de mantenimiento que desea eliminar y seleccione **Delete**.

> **Nota**
>
> Antes de eliminar tareas de mantenimiento, asegúrese de que todos los datos tengan una copia de seguridad.

15 Configurar la Consola de administración

En este capítulo, se proporciona información sobre cómo configurar los parámetros generales de GFI EventsManager, como las licencias del producto, las opciones de rendimiento y las actualizaciones del producto.

Temas de este capítulo:

15.1 Opciones de rendimiento 296

15.2 Actualizaciones del producto 297

15.3 Licencias del producto 305

15.4 Información de versión del producto 307

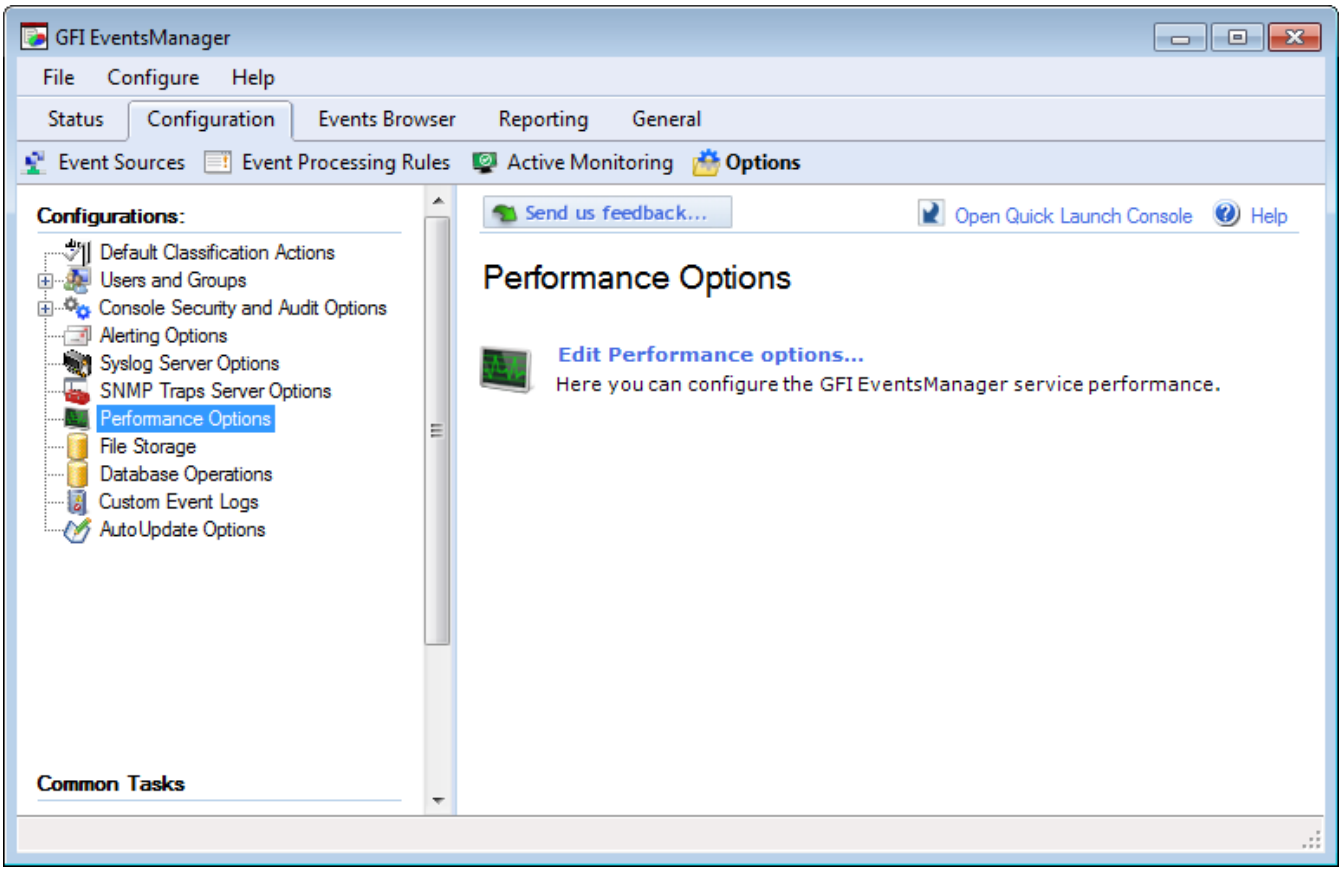
15.5 Importar y exportar configuraciones 308

15.6 Diseñar restricciones de consulta 314

15.1 Opciones de rendimiento

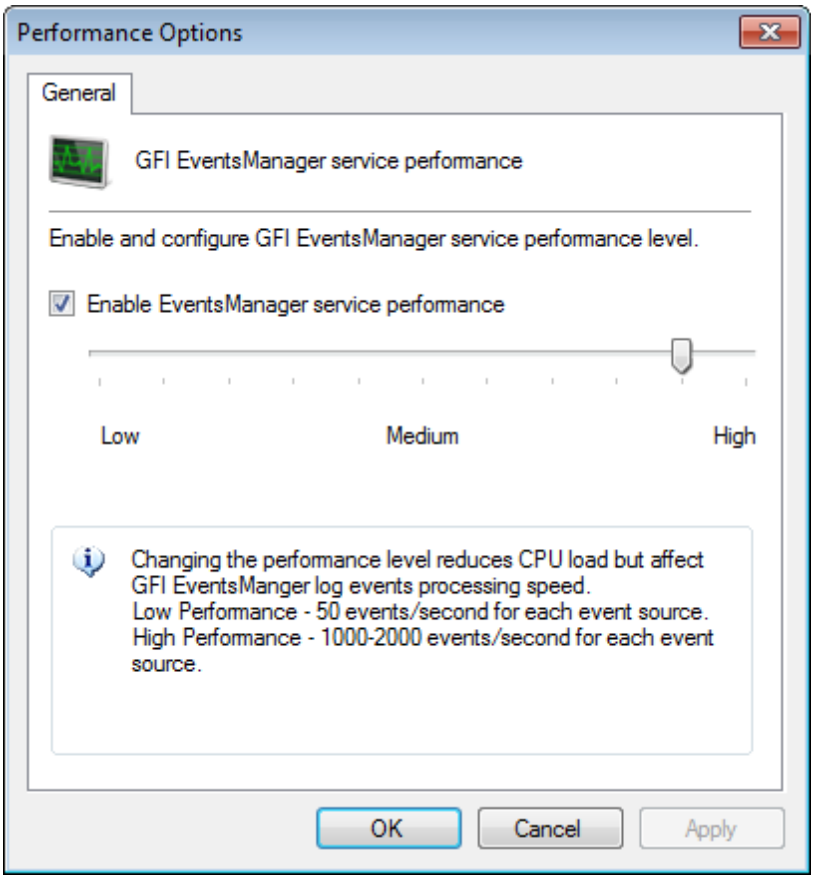
GFI EventsManager le proporciona opciones que le permiten definir el nivel de rendimiento del servicio de GFI EventsManager.

Para configurar el nivel de rendimiento:



Captura de pantalla 252: Opciones de rendimiento deGFI EventsManager

1. En la ficha **Configuration > Options > Configurations**, haga clic con el botón secundario en **Performance Options** y seleccione **Edit Performance Options**.


Performance Options
General
GFI EventsManager service performance
Enable and configure GFI EventsManager service performance level.
Enable EventsManager service performance
Low
Medium
High
Changing the performance level reduces CPU load but affect GFI EventsManger log events processing speed.
Low Performance - 50 events/second for each event source.
High Performance - 1000-2000 events/second for each event source.
OK
Cancel
Apply

Captura de pantalla 253: Cuadro de diálogo Performance Options

2. Marque o desmarque **Enable EventsManager service performance** para activar o desactivar las opciones de rendimiento del servicio.

3. Mueva el deslizador de izquierda (bajo) a derecha (alto) hasta que alcance el nivel de rendimiento requerido.

4. Haga clic en **Apply** y **OK**.

Nota

Se estima que definir el nivel de rendimiento en **low** procesa **50 eventos por segundo por origen de eventos**, mientras que definir la barra en **high** procesa **de 1000 a 2000 eventos por segundo por origen de eventos**.

15.2 Actualizaciones del producto

GFI publica actualizaciones del producto de forma periódica para mejorar o agregar funcionalidades a GFI EventsManager. Es importante descargar e instalar las actualizaciones del producto puesto que resuelven los problemas con tecnologías subyacentes, además de aumentar la compatibilidad con diferentes tecnologías y dispositivos.

Cuando el host de GFI EventsManager está conectado a Internet, se pueden descargar las actualizaciones de los productos directamente desde la Consola de administración. Cuando el acceso a Internet es limitado o nulo, se pueden descargar las actualizaciones del producto desde una

ubicación alternativa y, a continuación, se las puede colocar en el repositorio de actualizaciones de forma manual. Consulte las siguientes secciones para obtener información acerca de:

» Descargar actualizaciones directamente

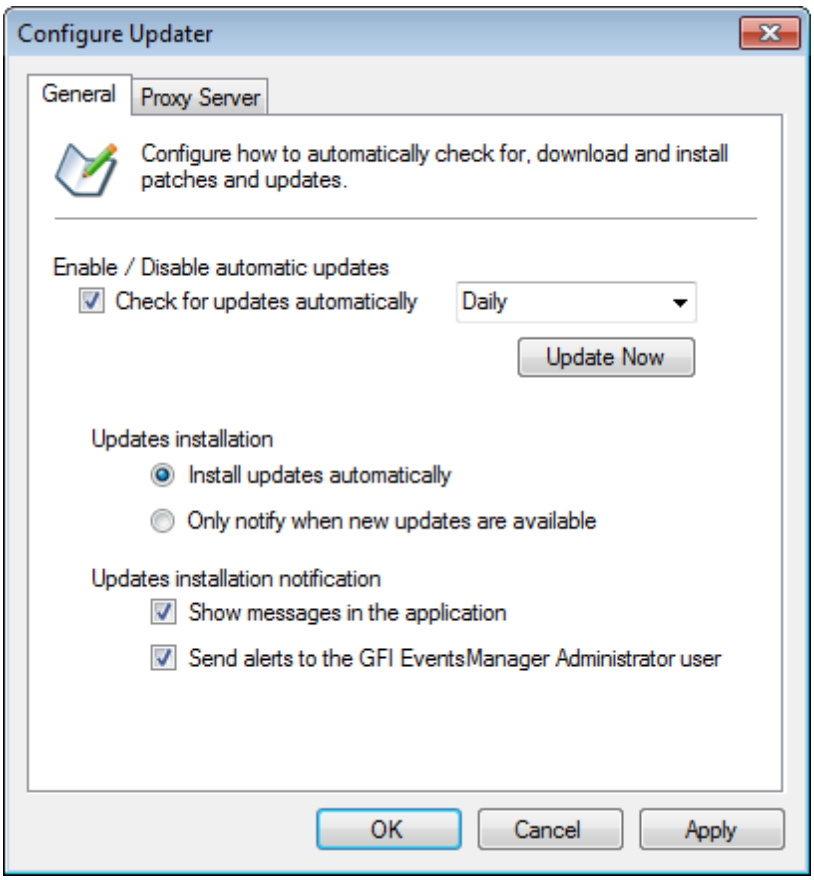
» Descargar actualizaciones desde una ubicación alternativa (sin conexión)

15.2.1 Descargar actualizaciones directamente

GFI EventsManager le permite a los usuarios configurar cómo comprobar, descargar e instalar de forma automática las actualizaciones del producto.

Para configurar las opciones de actualización automática:

1. En la ficha **Configuration > Options > Configurations**, haga clic con el botón secundario en **Auto Update Options** y seleccione **Edit updater options...**.



Captura de pantalla 254: Configurar opciones de actualización automática

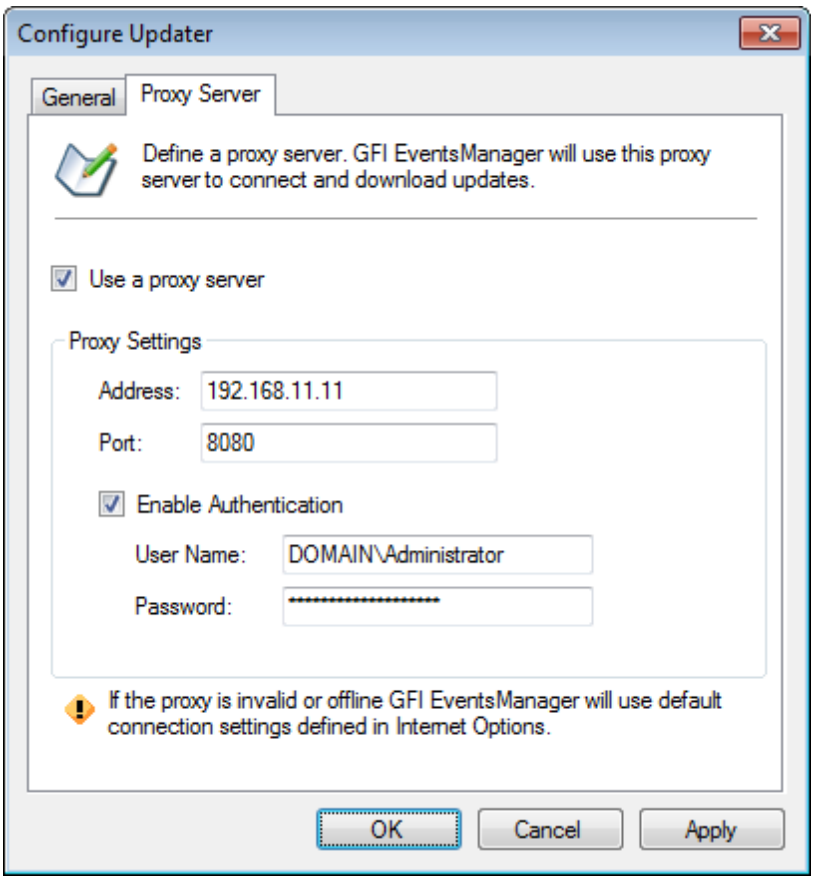
2. Configure las opciones que se describen a continuación:

Tabla 94: Opciones de actualización automática

Opciones	Descripción
Check for updates automatically	Si selecciona esta opción, GFI EventsManager comprobará automáticamente de forma diaria o semanal si hay actualizaciones.
Actualizar ahora	Si no se selecciona la opción **Check for updates automatically**, utilice esta opción para comprobar manualmente si hay actualizaciones e instalar las actualizaciones que faltan.
Install updates automatically	Instala automáticamente las actualizaciones descargadas.
Only notify me when updates are available	Las actualizaciones disponibles se muestran en la sección **Missing Updates**, pero no se instalan.

Opciones	Descripción
Show messages in the application	Muestra un mensaje en la parte inferior de la página de la aplicación. Haga clic en el mensaje que se muestra para iniciar las actualizaciones.
Send alerts on GFI EventsManager Administrator user	Envía una alerta por correo electrónico a la cuenta configurada del administrador de GFI EventsManager. Para obtener más información, consulte Configurar cuenta de administrador.

3. Si se deben descargar las actualizaciones del producto a través de un servidor proxy, haga clic en la ficha **Proxy Server**.



Captura de pantalla 255: Configurar el servidor proxy para descargar las actualizaciones del producto

4. Seleccione **Use a proxy server** y escriba la dirección del servidor proxy y el puerto de escucha en los campos **Address** y **Port**.

5. (Opcional) Si el servidor proxy requiere autenticación, seleccione **Enable Authentication** y escriba las credenciales de inicio de sesión del proxy.

6. Haga clic en **Apply** y **OK**.

15.2.2 Descargar actualizaciones desde una ubicación alternativa (sin conexión)

Para descargar actualizaciones del producto, GFI EventsManager se conecta al servidor de actualizaciones de GFI. Si el host de GFI EventsManager se encuentra en un entorno seguro y no está conectado a Internet, se pueden descargar las actualizaciones desde una ubicación alternativa.

Desde un equipo con acceso a Internet, descargue el paquete de actualizaciones y transfiéralo al host de GFI EventsManager. Utilice CMD para iniciar de forma manual una sesión de actualización mediante la herramienta de actualización provista en el directorio de instalación.

Necesitará un nombre de usuario y una contraseña para iniciar sesión en el servidor de actualizaciones de GFI. Para obtener sus credenciales de inicio de sesión, comuníquese con uno de

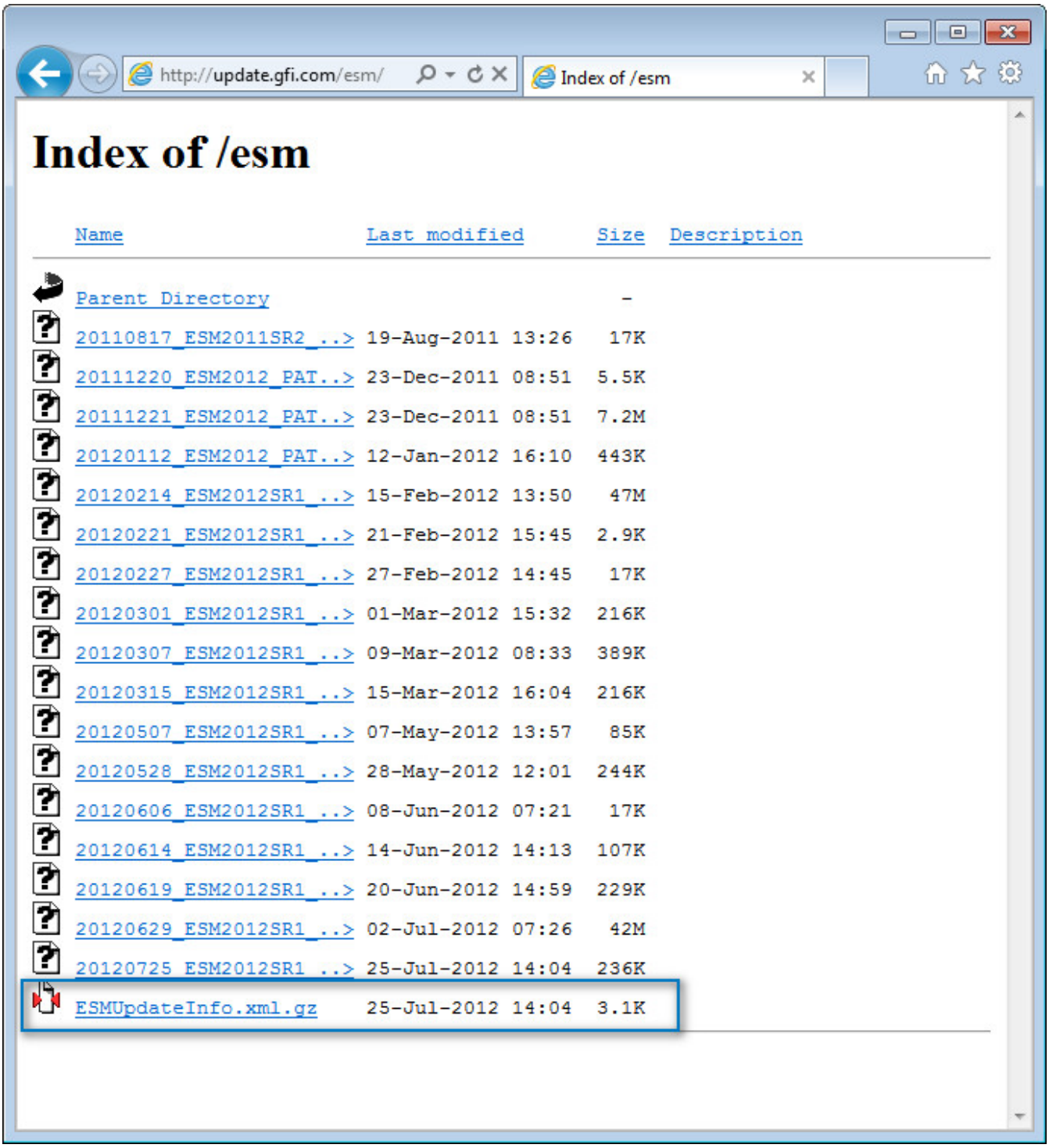
nuestros representantes de soporte. Para obtener más información, consulte Solicitar soporte técnico.

> **Nota**
>
> Este procedimiento supone que el producto está instalado en la ubicación predeterminada: **C:\Program Files (x86)\GFI\EventsManager2012**.

Para descargar las actualizaciones desde una ubicación alternativa:

1. En un equipo con acceso a Internet, vaya a http://update.gfi.com/esm.

2. Ingrese su nombre de usuario y contraseña. Se abre el directorio de actualizaciones de GFI EventsManager en el servidor de actualizaciones.

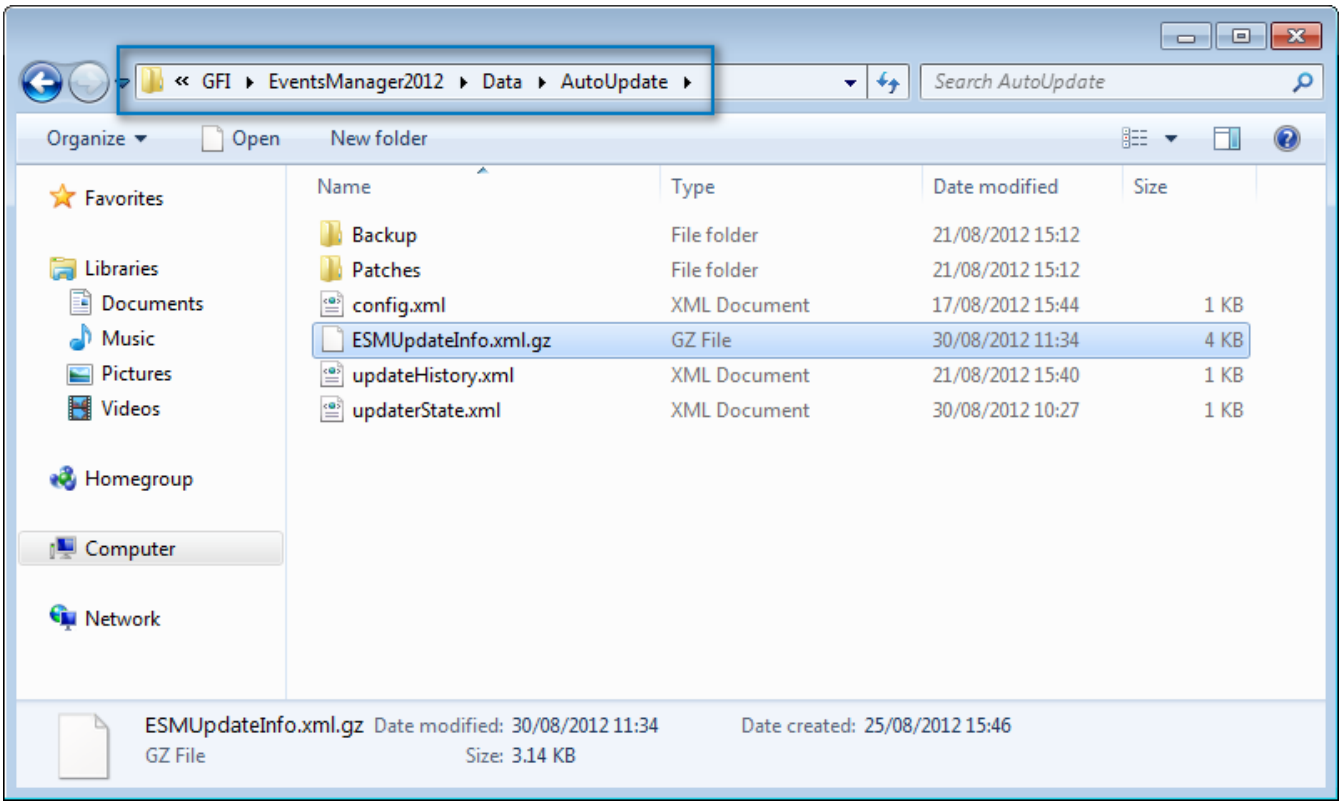


Captura de pantalla 256: Actualizaciones de GFI EventsManager

3. Haga clic en **ESMUpdateInfo.xml.gz** y guárdelo en una ubicación de su elección.

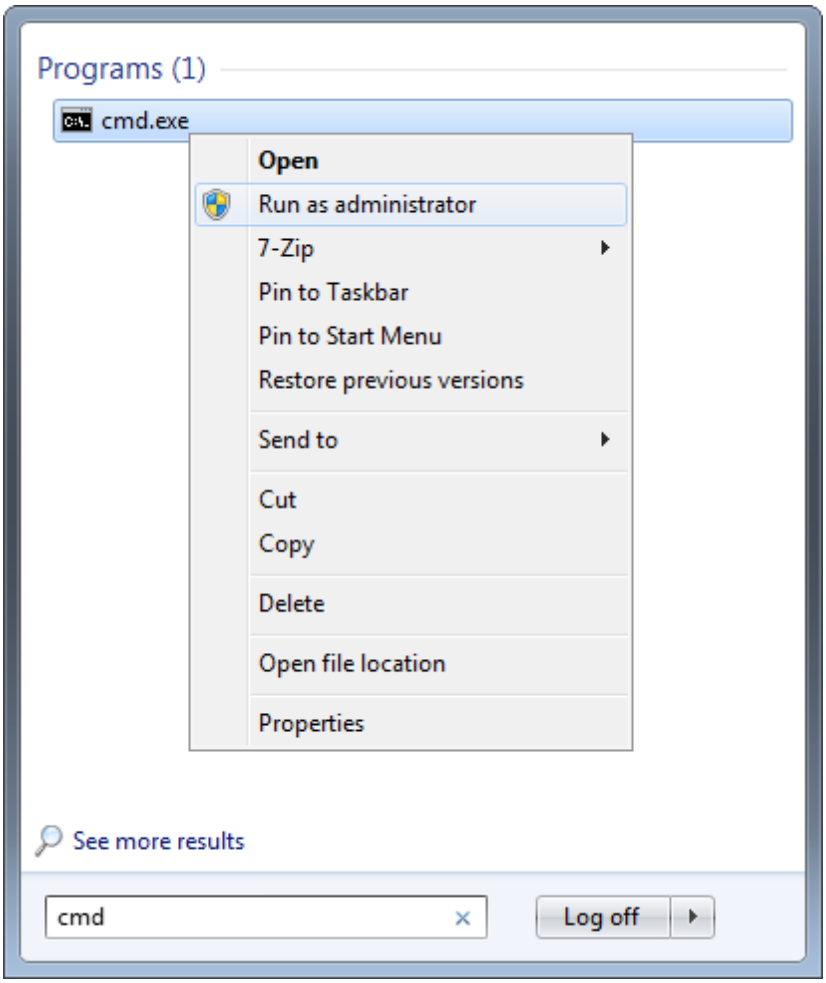
Nota

Transfiera el paquete de actualizaciones descargadas desde el equipo con acceso a Internet al host de GFI EventsManager.



Captura de pantalla 257: Repositorio de actualizaciones de GFI EventsManager

4. En el equipo con GFI EventsManager, copie el paquete de actualizaciones al siguiente repositorio: **C:\Program Files\GFI\EventsManager2012\Data\AutoUpdate**.

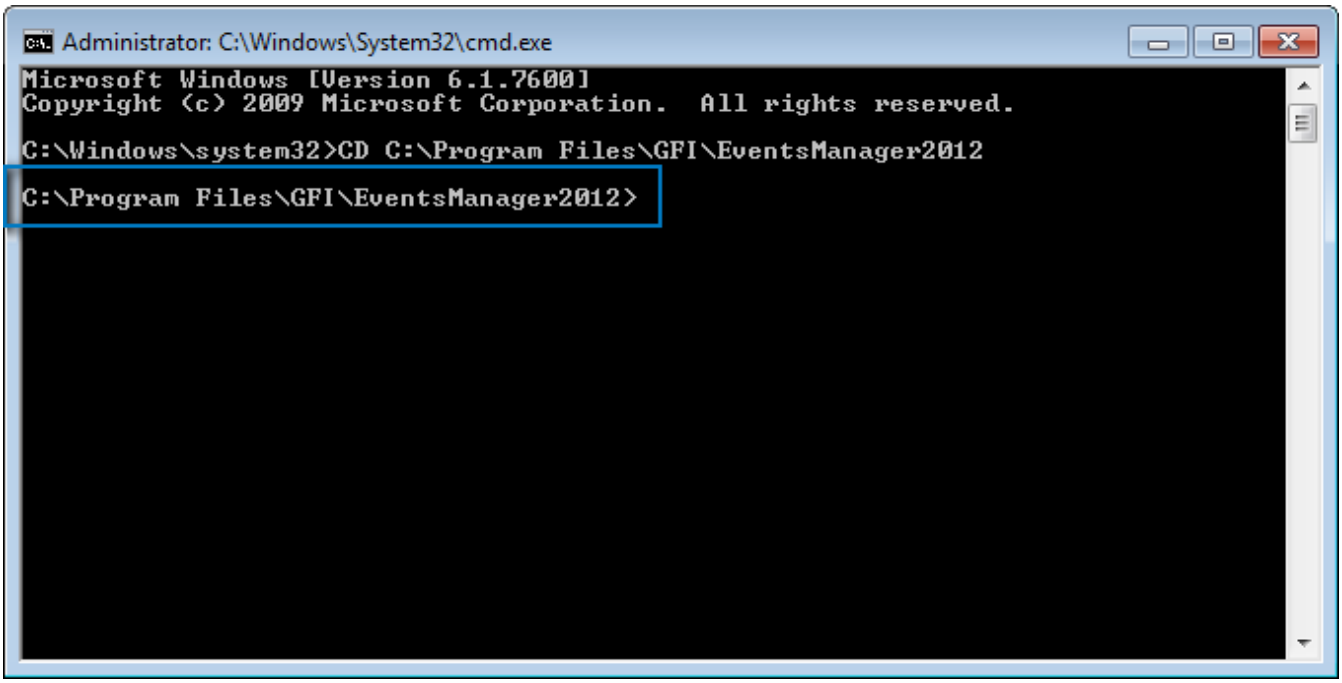


Captura de pantalla 258: Abrir CMD en el modo de administrador

5. Abra CMD en el modo de privilegios elevados y escriba:

- **sistemas de 64 bits:** `CD C:\Program Files (x86)\GFI\EventsManager2012`
- **sistemas de 32 bits:** `CD C:\Program Files\GFI\EventsManager2012`

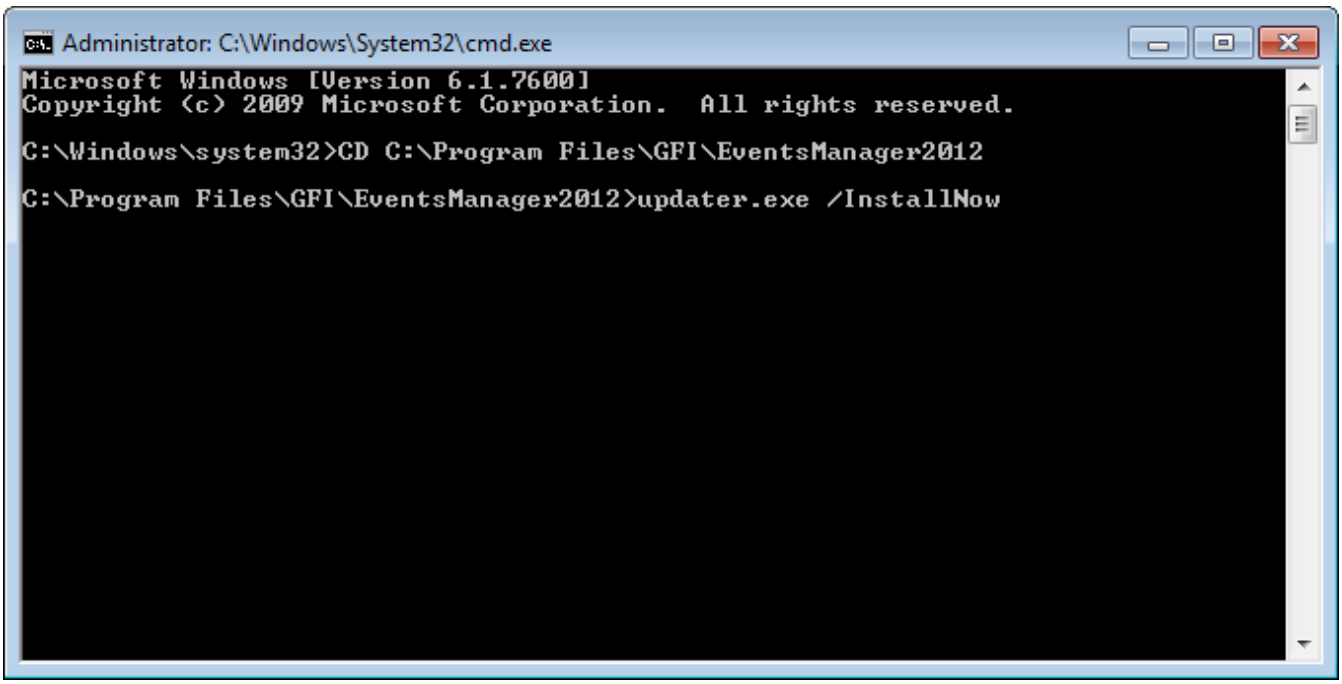
Presione la tecla **Enter**.



Captura de pantalla 259: Cambiar ruta de acceso al directorio de instalación de GFI EventsManager.

Nota

La ruta de acceso cambia según el directorio que especifique.


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>CD C:\Program Files\GFI\EventsManager2012
C:\Program Files\GFI\EventsManager2012>updater.exe /InstallNow

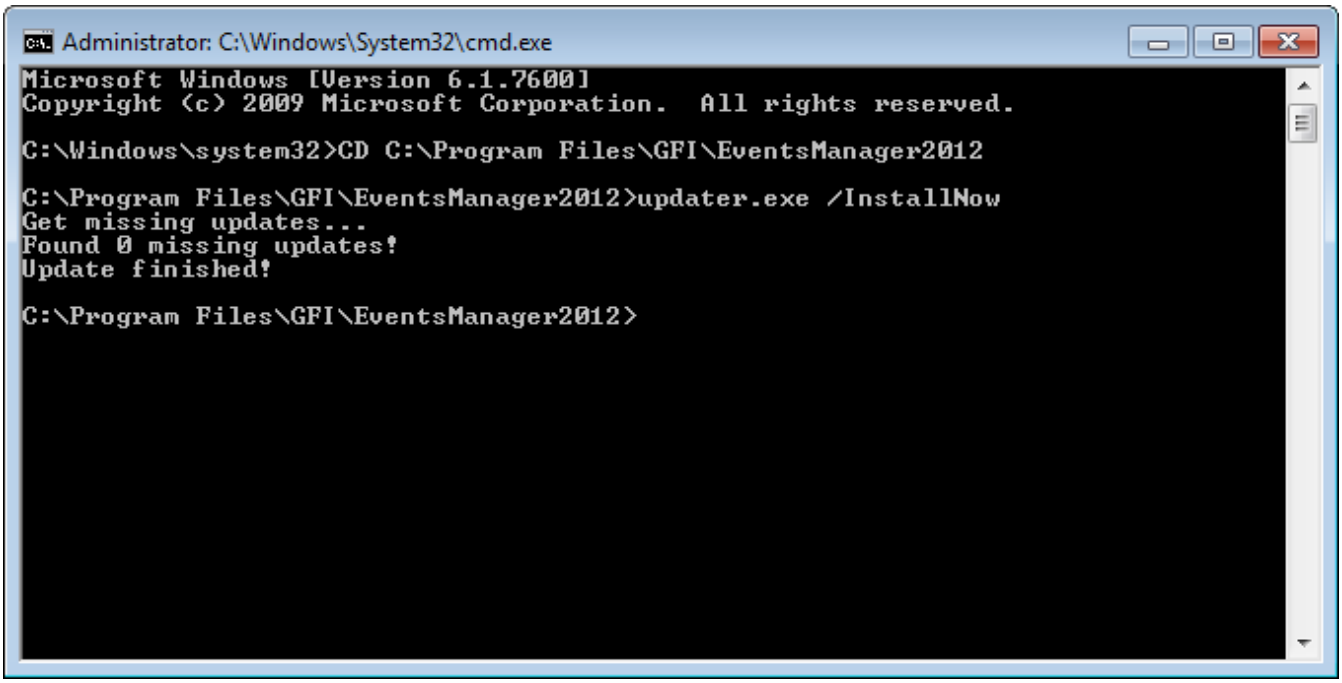
Captura de pantalla 260: Iniciar manualmente una sesión de actualización

6. Escriba:

```
updater.exe /InstallNow
```

Presione la tecla **Enter**.

Para asegurarse de que se hayan instalado todas las actualizaciones, ejecute `updater.exe /InstallNow` hasta que aparezca un mensaje que indique que se encontraron 0 actualizaciones faltantes.



Captura de pantalla 261: Estado de las actualizaciones

15.3 Licencias del producto

El equipo o el origen de eventos le concede licencia para usar GFI EventsManager. Se considera un origen de evento a todos los dispositivos que generan un registro. Consulte las secciones a continuación para obtener más información sobre las opciones de licencia de GFI EventsManager.

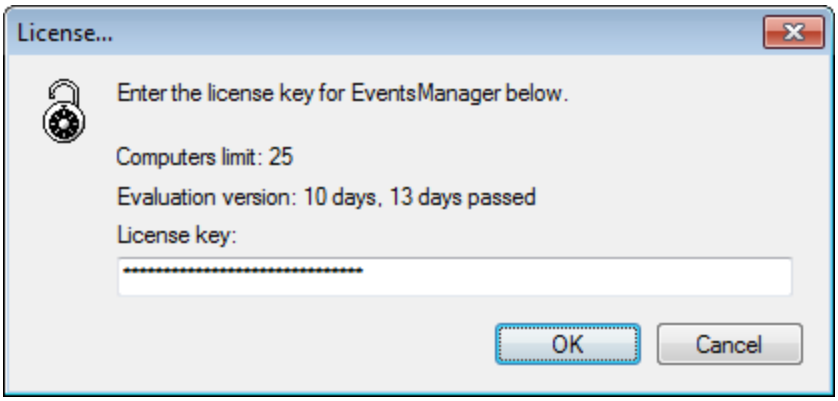
Las siguientes secciones contienen información acerca de:

- Actualizar la clave de licencia
- Obtener una clave de licencia de prueba de 30 días gratuita
- Ver detalles de la licencia
- Comprar una clave de licencia

15.3.1 Actualizar una clave de licencia

Para actualizar su clave de licencia actual:

1. En la ficha **General > General**, haga clic con el botón secundario en **Licensing** y seleccione **Update key...**.



Captura de pantalla 262: Cuadro de diálogo Update license key

3. Especifique su clave de licencia y haga clic en **OK**.

15.3.2 Obtener una clave de licencia de prueba de 30 días gratuita

GFI EventsManager le permite registrar su versión del producto y recibir una prueba gratuita de 30 días. Una vez transcurrido el período de prueba, se inhabilitan todos los servicios de supervisión de registros de eventos y de administración, y se necesita una clave de licencia completa.

Para registrarse y recibir una clave de licencia de prueba de 30 días:

1. En la ficha **General > General**, haga clic en **Licensing**.

2. Haga clic en el vínculo proporcionado. Será redireccionado a la página web de GFI, donde puede ingresar sus detalles y recibir la clave de licencia por correo electrónico. Se enviará su clave de prueba gratuita de 30 días a la dirección de correo electrónico que indique en el formulario de registro. Si tiene un sistema de filtro de correo no deseado, asegúrese de que el correo electrónico no esté bloqueado como correo no deseado.

15.3.3 Ver detalles de la licencia

Los detalles de la licencia le proporcionan detalles de la distribución de licencias. Para ver los detalles de la licencia:

1. En la ficha **General > General**, haga clic en **Licensing**.

2. En el panel derecho, haga clic en **Show details** para expandir la sección de detalles. Esto le mostrará el número de orígenes de eventos configurados y el tipo de licencia correspondiente servidor (por ejemplo, estación de trabajo o servidor).

15.3.4 Comprar una clave de licencia

Para adquirir una clave de licencia:

1. En la ficha **General > General**, haga clic en **Licensing**.

Captura de pantalla 263: Botón para comprar

2. En el panel derecho, haga clic en **Buy now!**. Será redireccionado a la página web de GFI, donde puede ver más información acerca de las licencias y la compra de una clave válida.

Nota

Para obtener más información, consulte:

- Información de licencias - http://www.gfi.com/page/13789/products/gfi-eventsmanager/pricing/licensing/licensing
- Información de precios -http://www.gfi.com/products/gfi-eventsmanager/pricing

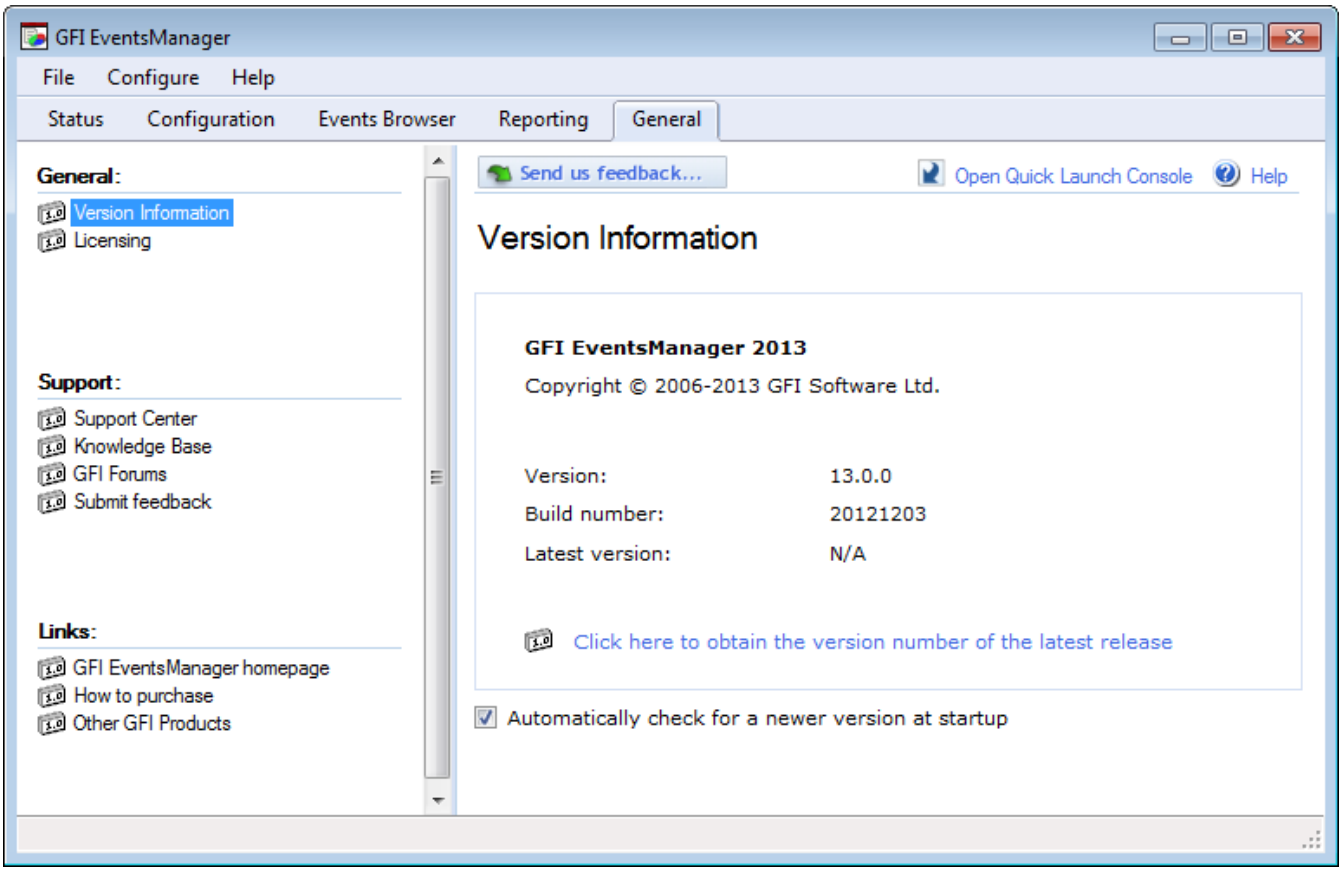
15.4 Información de versión del producto

GFI recomienda mantener GFI EventsManager actualizado y usar la última versión del producto para obtener compatibilidad integral con características y dispositivos. La información de la versión también puede ser útil para solucionar errores de funcionalidad con un representante de soporte técnico. Consulte las siguientes secciones para obtener información acerca de:

15.4.1 Comprobar su versión de GFI EventsManager

Para comprobar los detalles de información de su versión:

1. En la ficha **General > General**, haga clic en **Version Information**.



Captura de pantalla 264: Pantalla Version Information

2. Vea los detalles de la versión en el panel derecho.

3. (Opcional) Haga clic en **Click here to obtain the version number of the latest release** para obtener la información de versión más reciente de los servidores de GFI.

15.4.2 Comprobar si hay versiones nuevas

Para comprobar si hay nuevas compilaciones de GFI EventsManager:

1. En la ficha **General > General**, haga clic con el botón secundario en **Version Information** y seleccione **Check for newer builds...**.

2. (Opcional) En el panel derecho, marque o desmarque la opción **Automatically check for a newer version at startup** para comprobar de forma automática si hay nuevas versiones. Esta opción está marcada de forma predeterminada.

15.5 Importar y exportar configuraciones

La herramienta de importación y exportación le permite mover sin problemas las configuraciones de una instancia de GFI EventsManager a otra. Esto también se puede hacer como parte de un plan de recuperación ante desastres, para evitar tener que volver a configurar GFI EventsManager en caso de un desastre. Los siguientes parámetros se pueden importar/exportar por medio de GFI EventsManager:

- Orígenes de eventos
- Reglas de procesamiento de eventos
- Filtros del Explorador de eventos
- Opciones (entre las que se incluyen las acciones de clasificación predeterminadas, las opciones de alerta, las operaciones de base de datos y más).

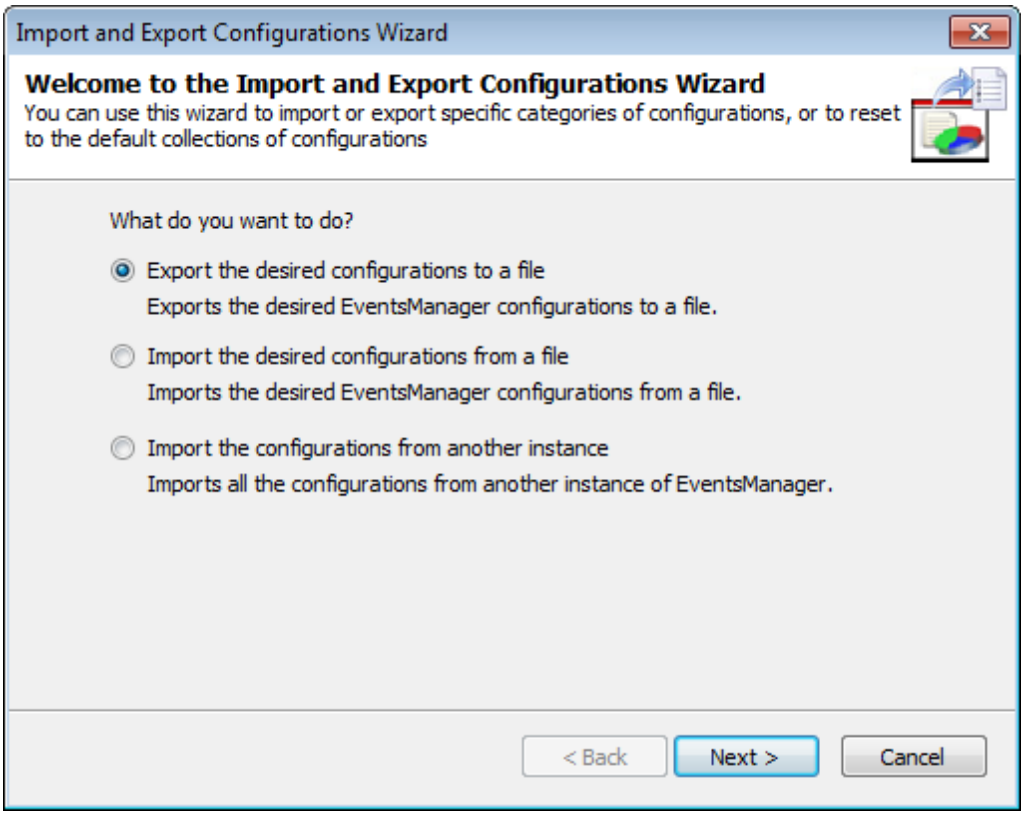
Esta sección contiene información acerca de:

- Exportar configuraciones a un archivo
- Importar configuraciones desde un archivo
- Importar configuraciones desde otra instancia

15.5.1 Exportar configuraciones a un archivo

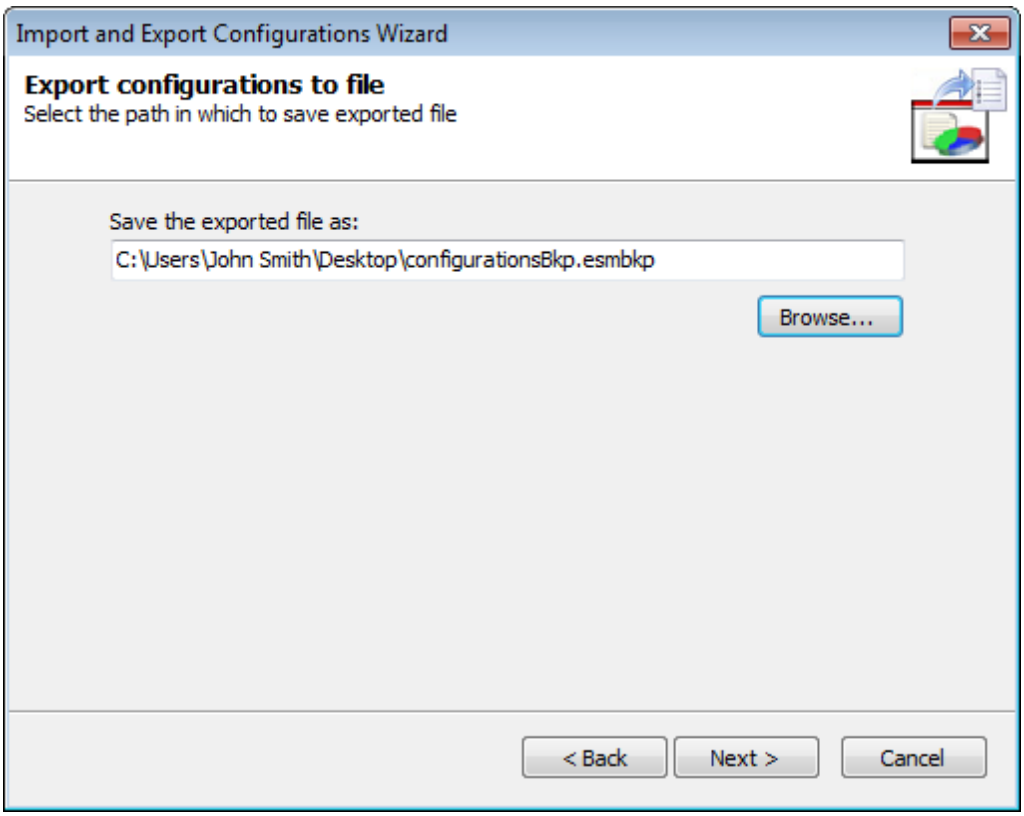
Para exportar sus configuraciones de GFI EventsManager:

1. Haga clic en **File > Import and Export Configurations...**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

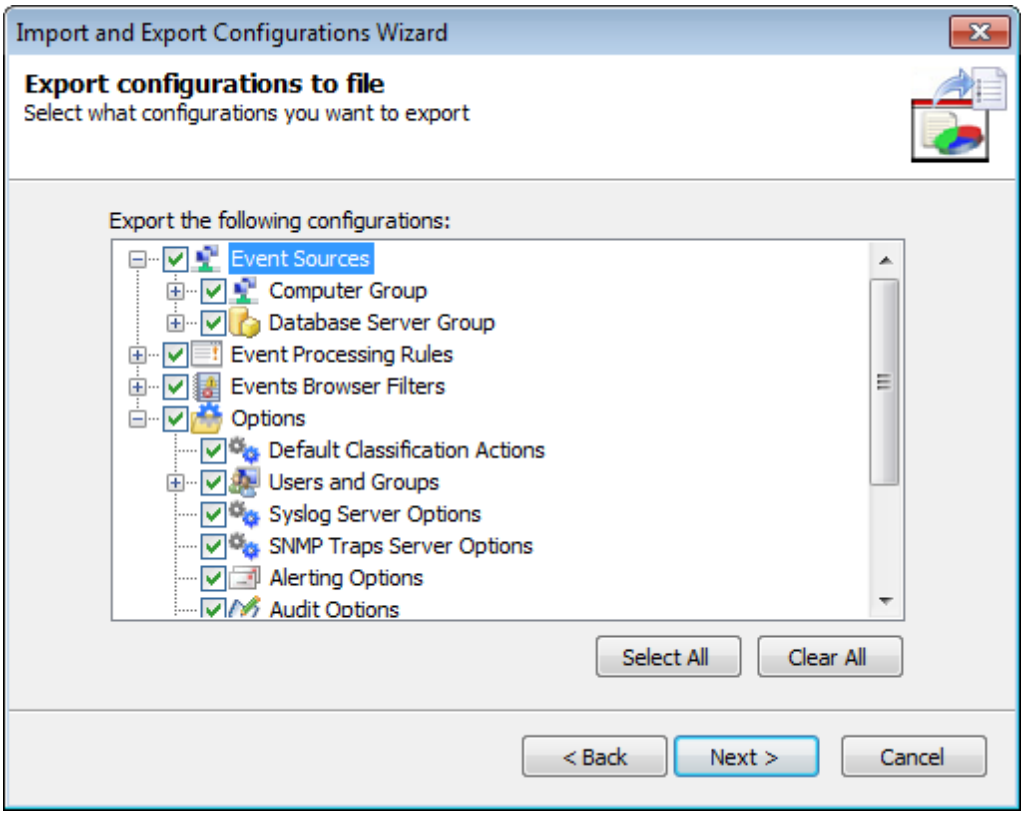
Captura de pantalla 265: Exportar configuraciones a un archivo

2. Seleccione **Export the desired configuration to a file** y haga clic en **Next**.



Captura de pantalla 266: Especificar destino de la exportación

3. Especifique la ubicación donde se guardará el archivo exportado o haga clic en **Browse...** para buscar la ubicación. Haga clic en **Siguiente**.



Captura de pantalla 267: Seleccionar configuraciones de exportación

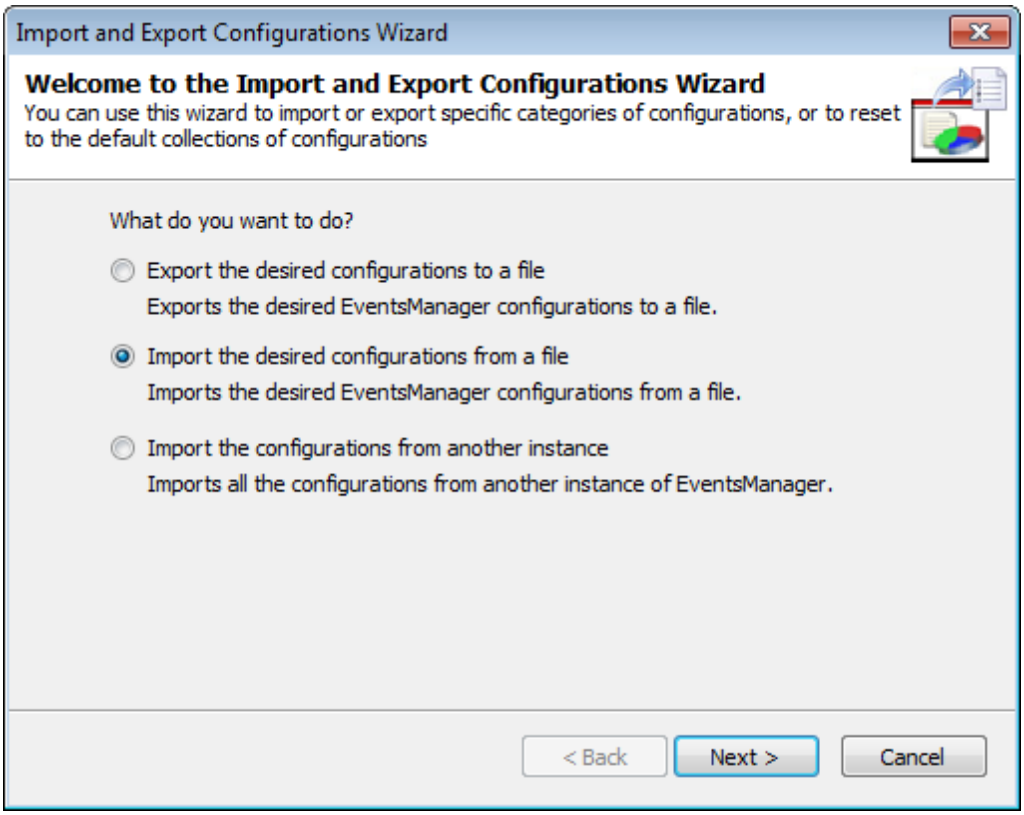
4. Seleccione las configuraciones que desea exportar y haga clic en **Next**.

5. Espere hasta que GFI EventsManager exporte la configuración y haga clic en **OK**.

15.5.2 Importar configuraciones desde un archivo

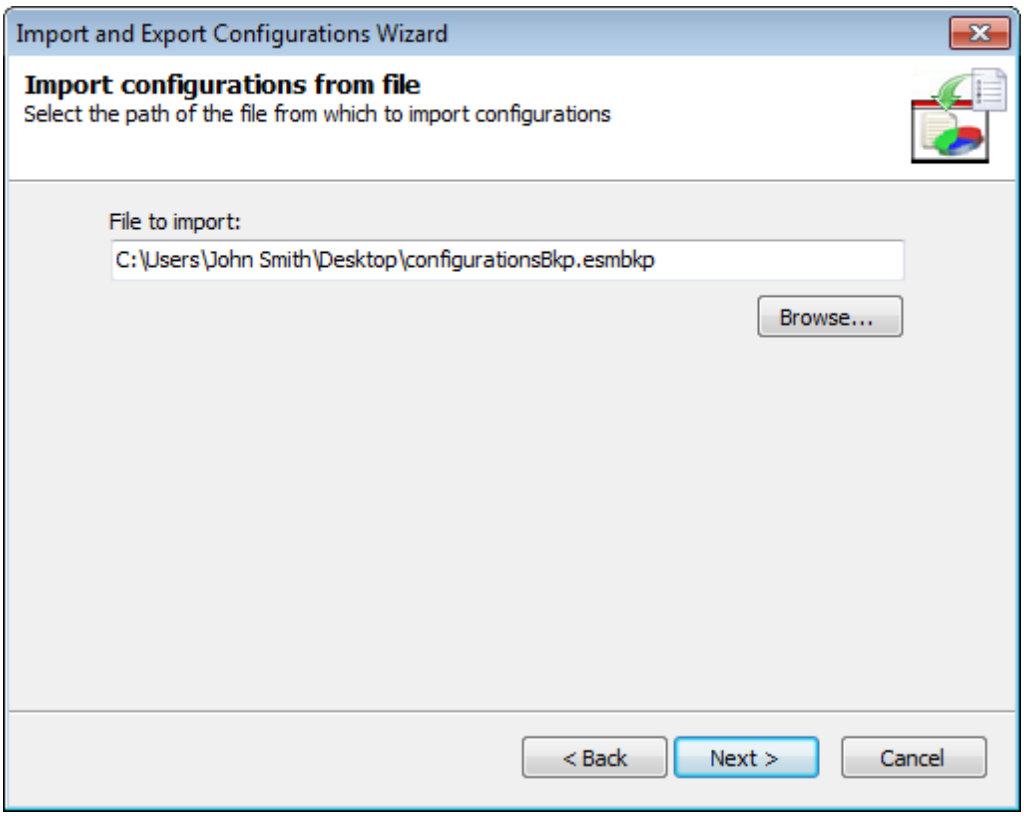
Para importar configuraciones desde un archivo:

1. Haga clic en **File > Import and Export Configurations...**.


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

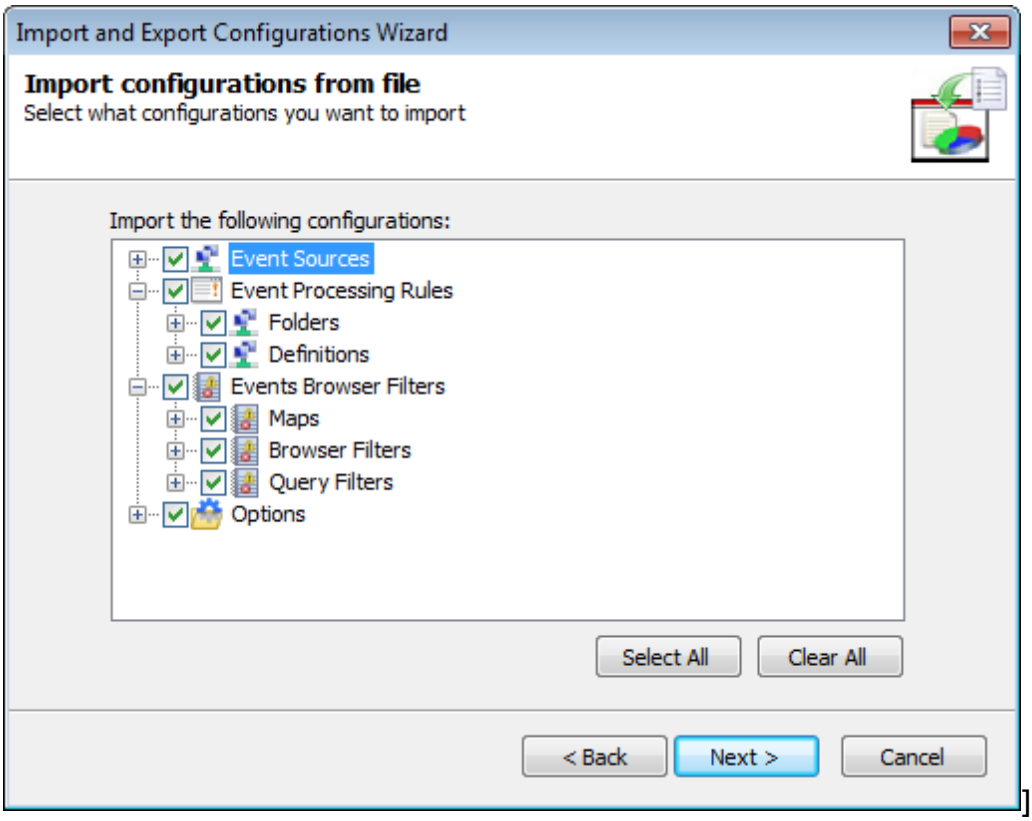
Captura de pantalla 268: Importar configuraciones desde un archivo

2. Seleccione **Import the desired configuration from a file** y haga clic en **Next**.



Captura de pantalla 269: Especificar ubicación del archivo de configuración

3. Especifique la ruta donde se almacena el archivo de importación o haga clic en **Browse...** para buscarlo. Haga clic en **Siguiente**.



Captura de pantalla 270: Seleccionar las configuraciones que desea importar

4. Seleccione la configuración que desea importar y haga clic en **Next**.

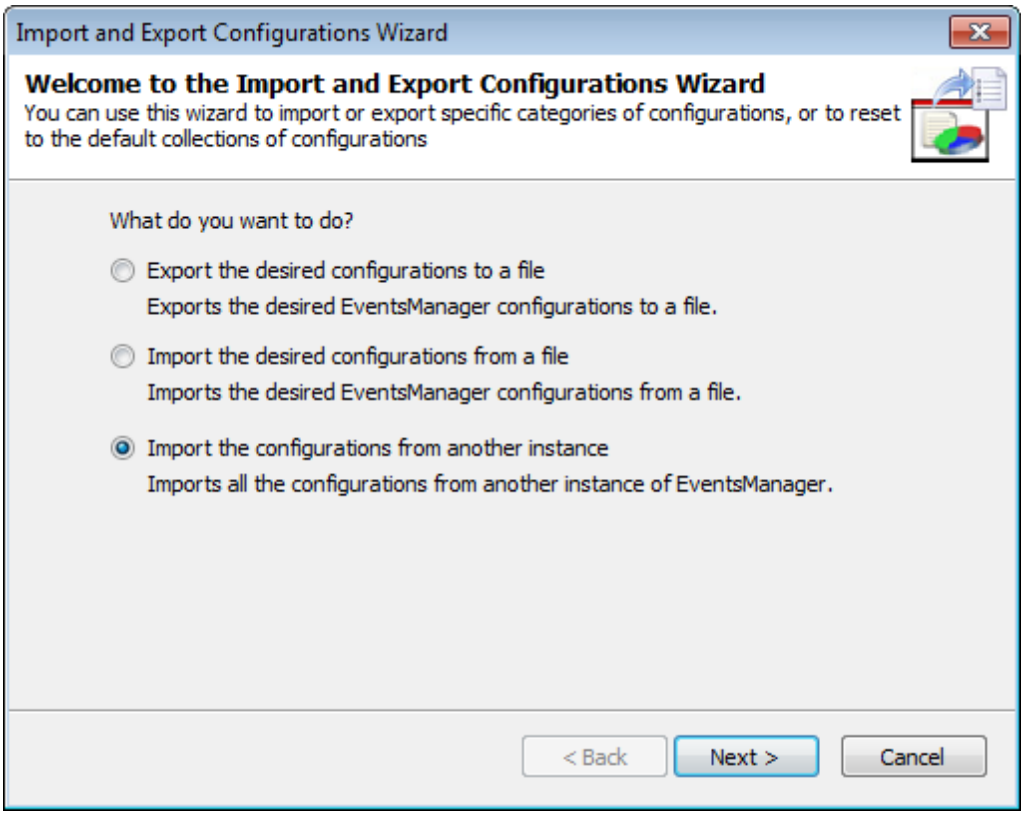
5. Espere hasta que GFI EventsManager importe las configuraciones y haga clic en **OK**.

> **Nota**
>
> Si GFI EventsManager detecta otras configuraciones, se le preguntará si desea reemplazar o combinar ambas configuraciones.

15.5.3 Importar configuraciones desde otra instancia

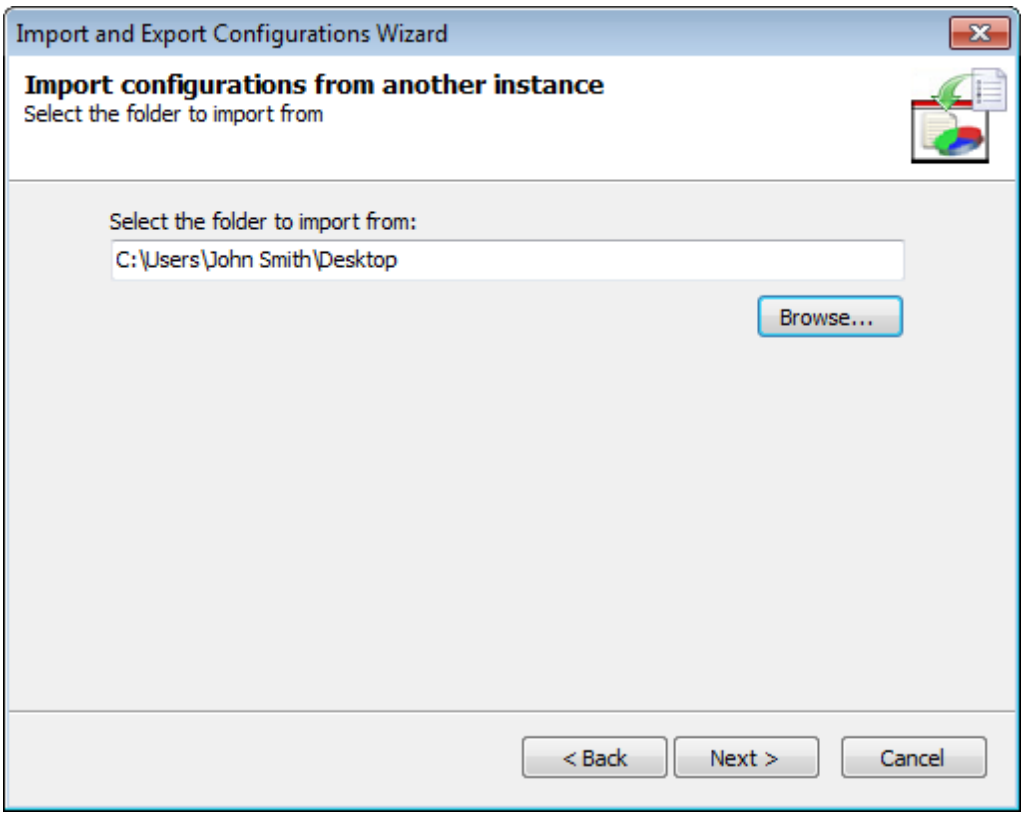
Para importar configuraciones desde otra instancia de GFI EventsManager:

1. Haga clic en **File > Import and Export Configurations...**


Import and Export Configurations Wizard
Welcome to the Import and Export Configurations Wizard
You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations
What do you want to do?
Export the desired configurations to a file
Exports the desired EventsManager configurations to a file.
Import the desired configurations from a file
Imports the desired EventsManager configurations from a file.
Import the configurations from another instance
Imports all the configurations from another instance of EventsManager.
< Back
Next >
Cancel

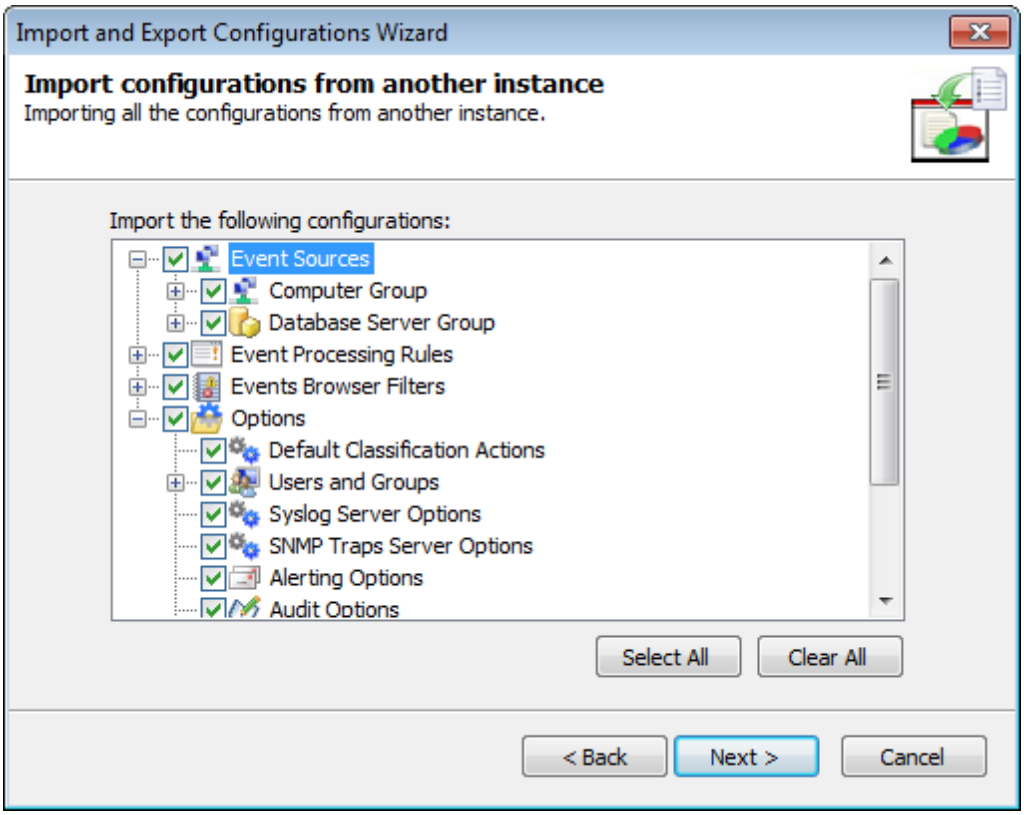
Captura de pantalla 271: Importar configuraciones desde otra instancia de GFI EventsManager

2. Seleccione **Import the configuration from another instance** y haga clic en **Next**.



Captura de pantalla 272: Especificar la ubicación de instancia

3. Especifique la ruta a la carpeta de instalación de la instancia desde la que desea importar configuraciones. O bien, haga clic en **Browse...** para buscarla. Haga clic en **Siguiente**.



Captura de pantalla 273: Seleccione las configuraciones que desea importar desde otra instancia de GFI EventsManager.

4. Seleccione la configuración que desea importar y haga clic en **Next**.

5. Espere hasta que la configuraciones se importen y haga clic en **OK**.

> **Nota**
>
> Si GFI EventsManager detecta otras configuraciones, se le preguntará si desea reemplazar o combinar ambas configuraciones.

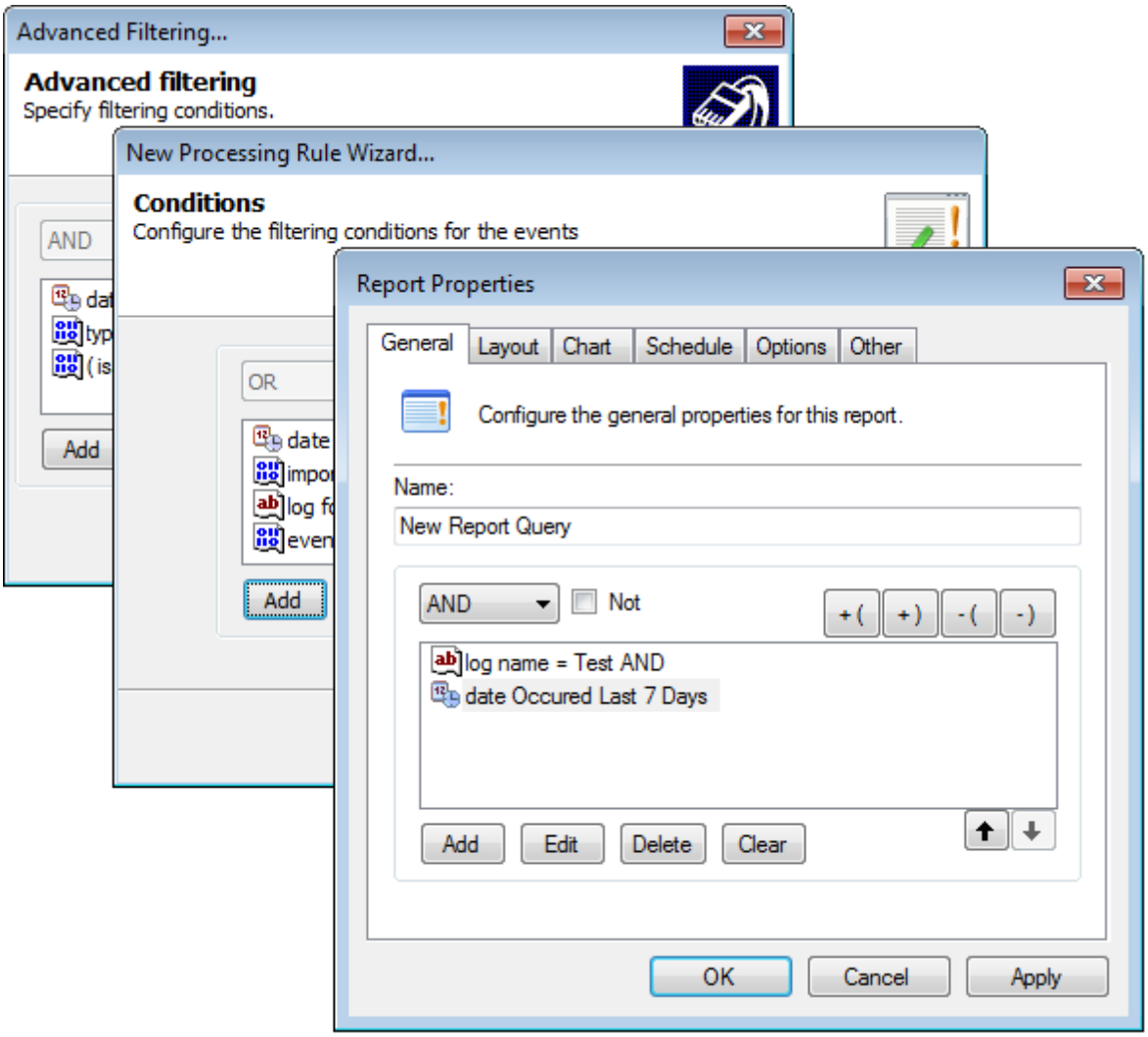
15.6 Diseñar restricciones de consulta

GFI EventsManager le permite crear consultas personalizadas mediante el cuadro de diálogo **Edit Query Restriction**. Las consultas son las instrucciones que GFI EventsManager envía al back-end de base de datos cuando almacena y recupera datos. También se utilizan para configurar reglas que permiten activar acciones y alertas cuando se detectan ciertos valores de atributos.

Los siguientes escenarios utilizan el cuadro de diálogo Edit Query Restriction para la configuración granular:

Tabla 95: Usos de restricciones de consulta

Uso	Descripción
Configuring reports	Permite crear consultas para filtrar la información del informe y generar informes relativos a atributos específicos.
Configuring user accounts	Impide que los usuarios de la Consola de administración de GFI EventsManager muestren información no autorizada sobre otros usuarios, registros de eventos o actividades de red.
Configuring events processing rules	Permite analizar los registros de eventos recopilados para detectar atributos que coincidan con los valores configurados en las consultas de procesamiento de eventos. Esto le permite inspeccionar la actividad de la red en detalle granular, lo cual le permite resolver los problemas relacionados con la red de forma proactiva antes de que se conviertan en problemas graves.



Captura de pantalla 274: Consultas de usuarios, reglas de procesamiento de eventos e informes

15.6.1 Usar el cuadro de diálogo Edit Query Restriction

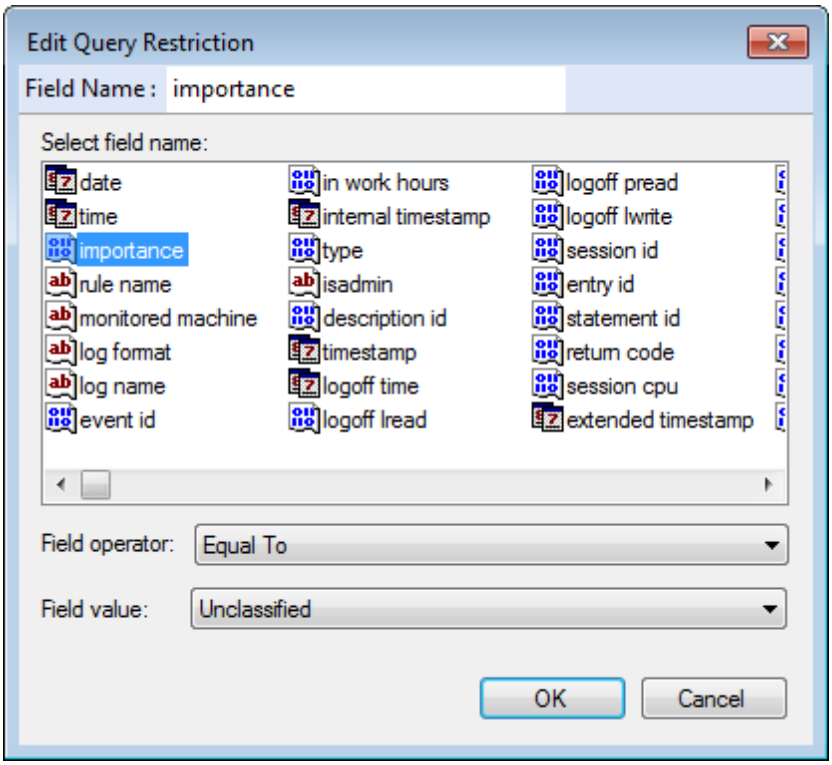
Para editar las restricciones de consulta para el filtrado y la configuración granulares:

1. En la siguiente tabla, se describe cómo iniciar el cuadro de diálogo Edit Query Restriction para usuarios, informes y reglas de procesamiento:

Tabla 96: Iniciar el cuadro de diálogo Edit Query Restrictions

Configurar...	Procedimiento
Usuarios	Para iniciar el cuadro de diálogo de restricciones de consulta: 1. Haga clic en la ficha **Configuration > Options > Users and Groups > Users**. 2. En el panel derecho, haga clic con el botón secundario en el usuario que desea editar y seleccione **Properties**. 3. En el cuadro de diálogo **User Properties**, haga clic en la ficha **Filter > Advanced...** 4. En el cuadro de diálogo **Advanced Filtering**, haga clic en **Add** para agregar.
Informes	Para iniciar el cuadro de diálogo de restricciones de consulta: 1. Haga clic en la ficha **Reporting**. 2. En la lista **Reports**, haga clic con el botón secundario en el informe que desea editar y seleccione **Properties**. 3. En la ficha **General**, haga clic en **Add**.

Configurar...	Procedimiento
Reglas de procesamiento de eventos	Para iniciar el cuadro de diálogo de restricciones de consulta: 1. Haga clic en la ficha **Configuration > Events Processing Rules**. 2. En la lista **Rule Folders**, haga clic con el botón secundario en la regla de procesamiento de eventos que desea editar y seleccione **Properties**. 3. En el cuadro de diálogo de propiedades de la regla de procesamiento, haga clic en la ficha **Conditions > Add**.



Captura de pantalla 275: Definir restricciones: Editar una restricción de consulta

2. En la lista de campos disponibles, seleccione un campo. Opcionalmente, escriba el nombre en el cuadro de texto **Field Name** para buscar el campo requerido.

3. Especifique un operador de campo en **Field Operator** para el campo seleccionado. Los operadores disponibles son:

Tabla 97: Definir restricciones: Operadores de campo

Operador de campo	Descripción
Equal To	Cuando el campo del evento es igual al valor configurado.
Less than	Cuando el campo del evento tiene un valor inferior al valor configurado.
Greater than	Cuando el campo del evento tiene un valor superior al valor configurado.
Occurred (Related to date/time fields)	Cuando la fecha del campo del evento ocurrió antes que la fecha del valor.
Like	Cuando el campo del evento tiene texto similar al texto del valor.
Contains	Cuando el campo del evento contiene el texto del valor.
Value in List	Cuando el campo del evento es igual a uno de los valores en una lista.

4. Especifique un valor en **Field Value** para el campo y el operador seleccionados. Algunos campos tienen valores predefinidos, mientras que otros requieren que se especifique un valor.

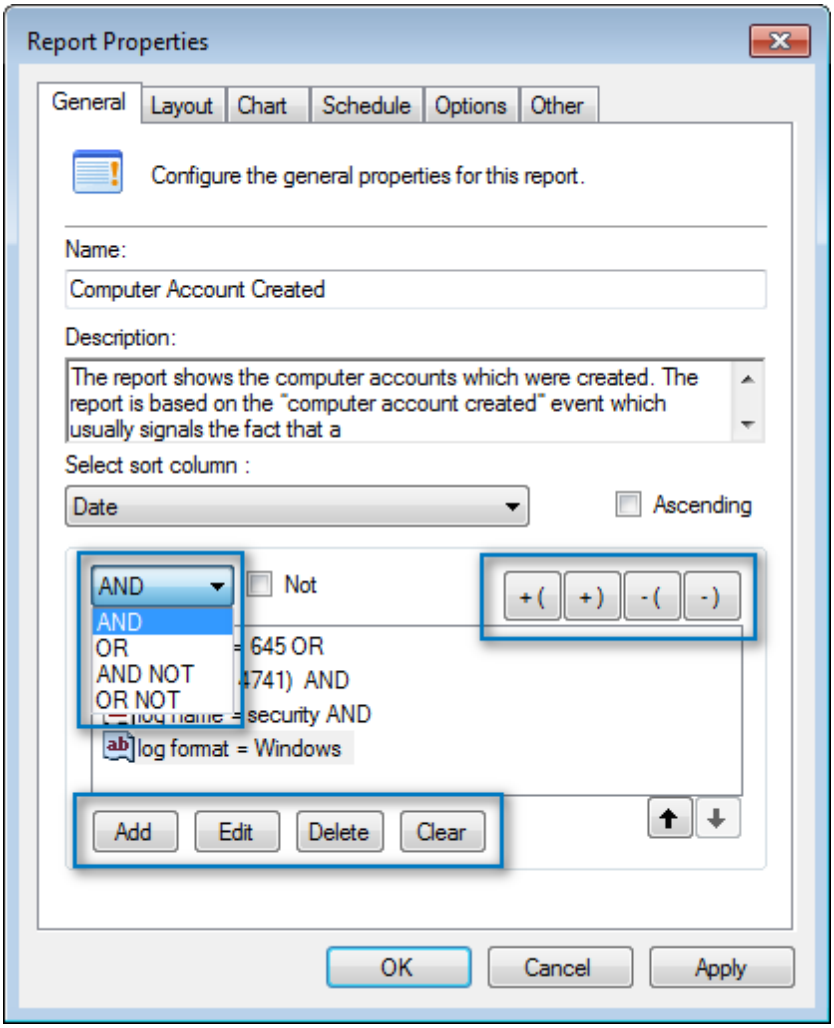
5. Haga clic en **OK** para aceptar.

Nota

Repita los Pasos 1 a 4 para agregar todos los campos que desea incluir en la consulta.

Nota

Puede copiar restricciones de informe de informes existentes. En la ficha **Reporting > Reports**, haga clic con el botón secundario en un informe y seleccione **Copy Report Restrictions**.



Captura de pantalla 276: Definir restricciones: Personalizar la condición

6. Una vez que estén definidas todas las restricciones, utilice las opciones que se describen a continuación para personalizar las condiciones de consulta:

Tabla 98: Definir restricciones: Herramientas de condición de consulta

Opciones	Descripción
AND	Seleccione la condición que desea configurar y seleccione AND. La condición seleccionada Y las condiciones siguientes se deben cumplir para que la consulta sea válida.
OR	Seleccione la condición que desea configurar y seleccione OR. La condición seleccionada O las condiciones siguientes se deben cumplir para que la consulta sea válida.

Opciones	Descripción
AND NOT	Seleccione la condición que desea configurar y seleccione AND NOT. Ello significa que la condición seleccionada debe coincidir con los parámetros de restricción, pero que las siguientes condiciones no lo deben hacer.
OR NOT	Seleccione la condición que desea configurar y seleccione OR NOT. Ello significa que la condición seleccionada debe coincidir con los parámetros de restricción o que las siguientes condiciones no lo deben hacer.
+ (	Haga clic en "+ (" para agregar un paréntesis de apertura a la condición seleccionada. Primero se procesan las condiciones encerradas entre paréntesis.
+)	Haga clic en "+)" para agregar un paréntesis de cierre a la condición seleccionada. Primero se procesan las condiciones encerradas entre paréntesis.
- (	Haga clic en "- (" para eliminar un paréntesis de apertura de la condición seleccionada.
-)	Haga clic en "-)" para eliminar un paréntesis de cierre de la condición seleccionada.
Add	Haga clic en Add para abrir el cuadro de diálogo de restricciones y agregar más campos a la condición.
Edit	Haga clic en Edit para obtener acceso al cuadro de diálogo de restricciones y personalizar la condición seleccionada.
Suprimir	Haga clic en Delete para eliminar una condición.
Clear	El botón Clear elimina todas las condiciones de consulta.
Flecha hacia arriba	Utilice la flecha hacia arriba para desplazar hacia arriba en la lista la condición seleccionada.
Flecha hacia abajo	Use la flecha hacia abajo para desplazar hacia abajo en la lista la condición seleccionada.

7. Haga clic en **Apply** y **OK**.

16 Herramientas de la línea de comandos

GFI EventsManager le proporciona herramientas de la línea de comandos a través de las cuales puede llevar a cabo diversas funciones sin tener acceso a la Consola de administración. Las herramientas CMD disponibles se encuentran en la carpeta de instalación de GFI EventsManager.

Temas de este capítulo:

16.1 Usar ESMCmdConfig.exe 319

16.2 Usar EsmDlibM.exe 322

16.3 Usar DLibAdm.exe 331

16.4 Usar EsmReport.exe 333

16.1 Usar ESMCmdConfig.exe

ESMCmdConfig.exe le permite configurar opciones generales para GFI EventsManager. Por ejemplo:

- Credenciales de inicio de sesión de GFI EventsManager
- Clave de licencia
- Configuración del servidor de correo
- Cuenta de administrador
- Crear/Eliminar accesos directos del grupo
- Obtener nombres de los equipos

Para utilizar ESMCmdConfig.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.
2. Haga clic en **Ctrl + Shift + Enter** para ejecutar CMD con privilegios elevados.
3. Cambie el directorio al directorio de instalación de GFI EventsManager. Ejemplo:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Escriba **ESMCmdConfig.exe** seguido de las funciones que se describen a continuación:

- /op:registerService
- /op:enable
- /op:disable
- /op:SetLicense
- /op:configureAlerting
- /op:setAdminEmail
- /op:createProgramGroupShortcuts
- /op:removeProgramGroupShortcuts
- /op:getComputers

16.1.1 /op:registerService

Esta función le permite registrar servicios deGFI EventsManager a través de una cuenta de administrador. Se admiten los siguientes parámetros:

Tabla 99: Parámetros de /op:registerService

Parámetro	Descripción
/username:<*nombre de usuario*>	Especifique el nombre de usuario de una cuenta de administrador. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/pass:<*contraseña*>	Especifique la contraseña de la cuenta especificada en el parámetro **/username**.

Ejemplo

```
ESMCmdConfig.exe /op:registerService /username:Domain\Administrator
/pass:p@ss
```

16.1.2 /op:enable

Esta función le permite activar las funciones de administración de eventos y no admite parámetros adicionales.

Ejemplo

```
ESMCmdConfig.exe /op:enable
```

16.1.3 /op:disable

Esta función le permite desactivar las características de administración de eventos y le solicita al usuario un mensaje personalizado. Se admite el siguiente parámetro:

Tabla 100: /op:disable Parameter

Parámetro	Descripción
/message: <*mensaje*>	Especifique un mensaje personalizado que se mostrará al usuario antes de que se inhabiliten las funciones de administración de eventos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
ESMCmdConfig.exe /op:disable /message:"Events Management Disabled!"
```

16.1.4 /op:SetLicense

Esta función le permite ingresar la clave de licencia del producto. Se admite el siguiente parámetro:

Tabla 101: Parámetros /op:SetLicense

Parámetro	Descripción
/licenseKey:<*clave*>	Especifique la clave de licencia del producto.

Ejemplo

```
ESMCmdConfig.exe /op:SetLicense /licenseKey:*********
```

16.1.5 /op:configureAlerting

Esta función le permite activar y configurar las opciones de alerta por correo electrónico. Se admiten los siguientes parámetros:

Tabla 102: Parámetros /op:configureAlerting

Parámetro	Descripción
/Server:<*servidor*>	Especifique la dirección IP del servidor de correo electrónico o el nombre de dominio completo (FQDN, por sus siglas en inglés).
/SenderEmail:<*correo electrónico*>	Especifique la dirección de correo electrónico del remitente. Parece que se enviaron las notificaciones desde la dirección especificada.
/Port:<*puerto*>	Especifique el puerto TCP que se utiliza para enviar mensajes de correo electrónico.
/RequiresAuthentication: <*true*|*false*>	Especifique si el servidor de correo requiere autenticación. Se admiten los siguientes valores: » True » False
/User:<*nombre de usuario*>	Especifique el nombre de usuario de la dirección de correo electrónico especificada en el parámetro **/SenderEmail**. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/Pass:<*contraseña*>	Especifique la contraseña para el nombre de usuario especificado en el parámetro **/User**.

Ejemplo

```
ESMCmdConfig.exe /op:configureAlerting /Server:192.168.11.11
/SenderEmail:jsmith@domain.com /Port:25 /RequiresAuthentication:True
/User:jsmith /Pass:p@ss
```

16.1.6 /op:setAdminEmail

Esta función le permite configurar la dirección de correo electrónico del administrador de EventsManager. Se admite el siguiente parámetro:

Tabla 103: Parámetro /op:setAdminEmail

Parámetro	Descripción
/email:<*correo electrónico*>	Especifique la dirección de correo electrónico del administrador de EventsManager.

Ejemplo

```
ESMCmdConfig.exe /op:setAdminEmail /email:esmadmin@domain.com
```

16.1.7 /op:createProgramGroupShortcuts

Esta función le permite crear accesos directos de grupo y no tiene parámetros adicionales.

Ejemplo

```
ESMCmdConfig.exe /op:createProgramGroupShortcuts
```

16.1.8 /op:removeProgramGroupShortcuts

Esta función le permite eliminar los accesos directos de grupo y no tiene parámetros adicionales.

Ejemplo

```
ESMCmdConfig.exe /op:removeProgramGroupShortcuts
```

16.1.9 /op:getComputers

Esta función le permite recuperar un archivo de texto que contenga los nombres de los orígenes de eventos que administra GFI EventsManager. Se admite el siguiente parámetro:

Tabla 104: Parámetro /op:getComputers

Parámetro	Descripción
/filename:<*nombre de archivo*>	Especifique la ruta de acceso completa donde se exporta el archivo de texto, incluido el nombre del archivo de texto. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
ESMCmdConfig.exe /op:getComputers /filename:C:\ComputerNames.txt
```

16.2 Usar EsmDlibM.exe

EsmDlibM.exe le permite ejecutar operaciones en el sistema de almacenamiento de archivos donde se almacenan los eventos procesados (base de datos back-end). Entre estas operaciones, se incluyen importar o exportar datos.

Para utilizar EsmDlibM.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.
2. Haga clic en **Ctrl + Shift + Enter** para ejecutar CMD con privilegios elevados.
3. Cambie el directorio al directorio de instalación de GFI EventsManager. Ejemplo:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Escriba **EsmDlibM.exe** seguido de las funciones que se describen a continuación:

- /importFromSQL
- /importFromDlib
- /copyData
- /importFromLegacyFile
- /exportToFile

- /importFromFile
- /commitDeletedRecords
- /exportToSQL

16.2.1 /importFromSQL

Esta función le permite importar datos de una base de datos SQL Server®. Se deben exportar los datos desde una versión anterior de GFI EventsManager. Se admiten los siguientes parámetros:

Tabla 105: Parámetros /importFromSQL

Parámetro	Descripción
/server:<*serverName*>	Especifique la dirección IP o el nombre de la máquina de SQL Server®.
/database:<*(maindb)|(backupdb)|databaseName*>	Especifique el tipo y el nombre de la base de datos de origen para importar los datos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
dbauth:<*SQL|WIN*>	Especifique el modo de autenticación configurado en el origen SQL Server®. Se admiten los siguientes valores: » **SQL**: para usar autenticación de SQL Server®. » **WIN**: para usar autenticación de Windows®.
/username:<*nombre_de_usuario*>	Especifique un nombre de usuario que tenga acceso a la base de datos desde la que desea importar los datos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	Especifique la contraseña del nombre de usuario especificado en el parámetro **/username**.
/anonpass1:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada, escriba la contraseña de anonimización primaria para descifrar los datos de importación.
/anonpass2:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada, con dos claves de anonimización, escriba en la contraseña de anonimización secundaria para descifrar los datos de importación.

Ejemplo

```
EsmDlibM.exe /importFromSQL /server:192.168.11.11
/database:EventsDatabase /dbauth:SQL /username:sa /password:p@ss
/anonpass1:p@ss
```

16.2.2 /importFromDlib

Esta función le permite importar datos que se exportaron desde un servidor de base de datos (DLIB, por sus siglas en inglés) de una versión anterior de GFI EventsManager. Se admiten los siguientes parámetros:

Tabla 106: Parámetros /importFromDlib

Parámetro	Descripción
/path:<*ruta*>	Especifique la ruta de acceso al servidor de base de datos DLib. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Parámetro	Descripción
/name:<*nombre*>	Especifique el nombre de la base de datos DLib que desea importar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/anonpass1:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada, escriba la contraseña de anonimización primaria para descifrar los datos de importación.
/anonpass2:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada, con dos claves de anonimización, escriba en la contraseña de anonimización secundaria para descifrar los datos de importación.

Ejemplo

```
EsmDlibM.exe /importFromDlib /path:C:\DLibServer /name:EventsData
/anonpass1:p@ss
```

16.2.3 /copyData

Esta función le permite copiar datos de un servidor de base de datos DLib a otro. Se admiten los siguientes parámetros:

Tabla 107: Parámetros /copyData

Parámetro	Descripción
/destinationPath:<*ruta_destino*>	Especifique el servidor de base de datos de destino. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/destinationName:<*nombre_destino*>	Especifique el nombre de la base de datos de destino. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/destinationEncPass:<*contraseña*>	(Opcional) Especifique una contraseña para cifrar los datos en el destino.
/sourcePath:<*ruta_origen*>	Especifique la ruta de acceso al servidor de base de datos de origen. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/sourceName:<*nombre_origen*>	Especifique el nombre de la base de datos de origen. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/sourceEncPass:<*contraseña*>	(Opcional) Especifique una clave de cifrado para cifrar los datos de origen.
/anonpass1:<*contraseña*>	(Opcional) Especifique la contraseña de anonimización primaria para anonimizar los datos de origen.
/anonpass2:<*contraseña*>	(Opcional) Especifique una contraseña de anonimización secundaria para anonimizar los datos de origen mediante el uso de dos claves.

Parámetro	Descripción
/period :<***tipo***><***número***><***unidad***>	Le permite filtrar por fecha de evento para acceder a los eventos desde el último día/semana/mes o desde un día/semana/mes anterior. Por ejemplo, para filtrar los eventos que ocurrieron en los últimos 24 días, el valor del parámetro es: **l24d**. Para filtrar los eventos con más de 3 semanas de antigüedad, el valor del parámetro es **O3W**. Se admiten los siguientes valores: » <type>: • **o**: anterior a • **l**: último/última » <number>: especifica la cantidad de días/semanas/meses » <unit>: • **d**: días • **w**: semanas • **m**: meses
/markEventsAsDeleted	(Opcional) Marca los eventos copiados como eliminados de la base de datos de origen. Estos eventos ya no se mostrarán en la Consola de administración, pero permanecerán en la base de datos. Para eliminarlos por completo de la base de datos, ejecute la tarea **Commit Deletions**.
/log_format:***<valor>*** /machine:***<valor>*** /importance:<valor> /occured:***<valor>***	Estos parámetros proporcionan al usuario una forma práctica para filtrar los eventos por las columnas correspondientes. Estos filtros son opcionales. Cuando se usan en conjunto, están vinculados a una condición AND en los datos de origen. A excepción de la máquina, donde el usuario puede ingresar el nombre de la máquina de destino según se muestra en el explorador de eventos, los demás parámetros tienen valores predefinidos de significado obvio, que se indican a continuación. Se admiten los siguientes valores: » log_format: • "windows • sql audit, para auditoría de sql • oracle audit, para auditoría de oracle • text logs, para registros de texto • syslog messages, para mensajes syslog • snmp traps, para capturas SNMP • monitoring, para supervisión » importance, para importancia • unclassified, para sin clasificar • low, para baja • medium, para media • high, para alta • critical, para crítica • noise, para ruido » ocurred • today, para el día de hoy • yesterday, para ayer • last 7 days, para los últimos 7 días • last 30 days, para los últimos 30 días • this month, para este mes • last month, para el mes pasado

Ejemplo

```
EsmDlibM.exe /copyData /destinationPath:Z:\DestServ
/destinationName:DestData /sourcePath:C:\SourServ
/sourceName:SourData /sourceEncPass:p@ss /markEventsAsDeleted
```

16.2.4 /importFromLegacyFile

Esta función le permite importar datos que se exportaron a archivos desde una versión anterior de GFI EventsManager. Se admiten los siguientes parámetros:

Tabla 108: Parámetros /importFromLegacyFile

Parámetro	Descripción
/path:<*ruta*>	Especifique la ruta de acceso al archivo de importación. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/logTypes:<*aplicación, personalizado, directorio, seguridad, dns, replicación de archivo, syslog, sistema, snmp, oracle, sql, texto*>	(Opcional) Especifique el tipo de registro que desea importar. Excluya el parámetro para importar todos los tipos de registro.
/password:<*contraseña*>	(Opcional) Especifique una contraseña para descifrar los datos de importación.
/anonpass1:<*contraseña*>	(Opcional) Especifique la contraseña de anonimización primaria para anonimizar los datos de importación.
/anonpass2:<*contraseña*>	(Opcional) Especifique una contraseña de anonimización secundaria para anonimizar los datos de importación mediante dos claves.

Ejemplo

```
EsmDlibM.exe /importFromLegacyFile
/path:C:\ImportData\Configuration.cfg /password:p@ss /anonpass1:p@ss
```

16.2.5 /exportToFile

Esta función le permite exportar datos desde un servidor de bases de datos DLib hasta otro como parte del proceso de centralización de datos. También puede utilizar esta función para obtener copias de seguridad de sus datos con fines de protección. Se admiten los siguientes parámetros:

Tabla 109: /exportToFile

Parámetro	Descripción
/path:<*ruta*>	Especifique la ruta de la carpeta donde se exportan los datos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/sourceEncPass:<*contraseña*>	(Opcional) Especifique una contraseña para cifrar los datos de origen.
/destinationEncPass:<*contraseña*>	(Opcional) Especifique una contraseña para cifrar los datos de destino.
/anonpass1:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada, escriba la contraseña de anonimización primaria para descifrar los datos exportados.

Parámetro	Descripción
/anonpass2:<*contra-seña*>	(Opcional) Si la base de datos de origen está anonimizada con dos claves de anonimización, escriba la contraseña de anonimización secundaria para descifrar los datos exportados.
/period :<*tipo*><*número*><*unidad*>	Le permite filtrar por fecha de evento para acceder a los eventos desde el último día/semana/mes o desde un día/semana/mes anterior. Por ejemplo, para filtrar los eventos que ocurrieron en los últimos 24 días, el valor del parámetro es: **l24d**. Para filtrar los eventos con más de 3 semanas de antigüedad, el valor del parámetro es **O3W**. Se admiten los siguientes valores: » <type>: • **o**: anterior a • **l**: último/última » <number>: especifica la cantidad de días/semanas/meses » <unit>: • **d**: días • **w**: semanas • **m**: meses
/markEventsAsDeleted	(Opcional) Marca los eventos copiados como eliminados de la base de datos de origen. Estos eventos ya no se mostrarán en la Consola de administración, pero permanecerán en la base de datos. Para eliminarlos por completo de la base de datos, ejecute la tarea **Commit Deletions**.

Parámetro	Descripción
/log_format:***<valor>*** /machine:***<valor>*** /importance:<valor> /ocured:***<valor>***	Estos parámetros proporcionan al usuario una forma práctica para filtrar los eventos por las columnas correspondientes. Estos filtros son opcionales. Cuando se usan en conjunto, están vinculados a una condición AND en los datos de origen. A excepción de la máquina, donde el usuario puede ingresar el nombre de la máquina de destino según se muestra en el explorador de eventos, los demás parámetros tienen valores predefinidos de significado obvio, que se indican a continuación. Se admiten los siguientes valores: » log_format: • "windows • auditoría de sql • auditoría de oracle • registros de texto • mensajes syslog • capturas SNMP • supervisión » importancia • Sin clasificar • Baja • Media • Alta • Crítica • Ruido » ocurred • Hoy • Ayer • Últimos 7 días • Últimos 30 días • Este mes • Mes pasado

Ejemplo

```
EsmDlibM.exe /exportToFile /path:C:\ExportedDataFolder
/sourceEncPass:p@ss /markEventsAsDeleted /importance:High
```

16.2.6 /importFromFile

Esta función le permite importar datos de un archivo como parte del proceso de centralización de datos. El archivo de importación se debe crear a partir de una tarea **Export to File**. Se admiten los siguientes parámetros:

Tabla 110: Parámetros /importFromFile

Parámetro	Descripción
/path:<*ruta*>	Especifique la ruta de acceso donde se guarda el archivo de importación. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	(Opcional) Si el archivo de importación está protegido con una contraseña, escriba la contraseña.
/log_format: **<*valor*>** /machine: **<*valor*>** /importance: <valor> /occured: **<*valor*>**	Estos parámetros proporcionan al usuario una forma práctica para filtrar los eventos por las columnas correspondientes. Estos filtros son opcionales. Cuando se usan en conjunto, están vinculados a una condición AND en los datos de origen. A excepción de la máquina, donde el usuario puede ingresar el nombre de la máquina de destino según se muestra en el explorador de eventos, los demás parámetros tienen valores predefinidos de significado obvio, que se indican a continuación. Se admiten los siguientes valores: » log_format: • "windows • auditoría de sql • auditoría de oracle • registros de texto • mensajes syslog • capturas SNMP • supervisión » importancia • Sin clasificar • Baja • Media • Alta • Crítica • Ruido » ocurred • Hoy • Ayer • Últimos 7 días • Últimos 30 días • Este mes • Mes pasado

Ejemplo

```
EsmDlibM.exe /importFromFile /path:C:\ImportFolder\Import.cfg
/password:p@ss /machine:MS11.domain.com /occured:true
```

16.2.7 /commitDeletedRecords

Esta función le permite eliminar los eventos que están marcados como eliminados de la base de datos. Se admiten los siguientes parámetros:

Tabla 111: Parámetros /commitDeletedRecords

Parámetro	Descripción
/dbPath:<*ruta_base_datos*>	Especifique la ruta de acceso al servidor de bases de datos que contiene los eventos marcados como eliminados. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	(Opcional) Si la base de datos está protegida por una contraseña, escriba la contraseña.
/anonpass1:<*contraseña*>	(Opcional) Si la base de datos está anonimizada, escriba la contraseña para quitar la anonimización.
/anonpass2:<*contraseña*>	(Opcional) Si la base de datos está anonimizada mediante dos claves de anonimización, escriba la clave secundaria.

Ejemplo

```
EsmDlibM.exe /commitDeletedRecords /dbpath:C:\DatabaseServerFolder
/password:p@ss /anonpass1:pa$$
```

16.2.8 /exoportToSQL

Esta función le permite exportar el evento especificado a SQL Server®. Se admiten los siguientes parámetros:

Tabla 112: Parámetros /exportToSQL

Parámetro	Descripción
/server:<*nombre_servidor*>	Especifique la dirección IP o el nombre del equipo que ejecuta SQL Server®. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/database:<*bd_principal|copia_seguridad_bd*>	Especifique el nombre de la base de datos de destino. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/dbauth:<*SQL|WIN*>	Especifique el modo de autenticación configurado en el origen SQL Server®. Se admiten los siguientes valores: » **SQL**: para usar autenticación de SQL Server®. » **WIN**: para usar autenticación de Windows®.
/username:<*nombre_usuario*	Especifique un nombre de usuario que tenga acceso a la base de datos desde la que desea importar los datos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	Especifique la contraseña del nombre de usuario especificado en el parámetro **/username**.

Parámetro	Descripción
/table:<*tabla*>	Especifique el nombre de la tabla de destino. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/period:<*tipo*><*número*><*unidad*>	Le permite filtrar por fecha de evento para acceder a los eventos desde el último día/semana/mes o desde un día/semana/mes anterior. Por ejemplo, para filtrar los eventos que ocurrieron en los últimos 24 días, el valor del parámetro es: **l24d**. Para filtrar los eventos con más de 3 semanas de antigüedad, el valor del parámetro es **O3W**. Se admiten los siguientes valores: » <type>: • **o**: anterior a • **l**: último/última » <number>: especifica la cantidad de días/semanas/meses » <unit>: • **d**: días • **w**: semanas • **m**: meses
/sourceEncPass:<*contraseña*>	(Opcional) Si los datos de origen se encuentran cifrados, escriba la contraseña para descifrar los datos exportados.
/anonpass1:<*contraseña*	(Opcional) Si la base de datos de origen está anonimizada, escriba la contraseña de anonimización primaria para descifrar los datos exportados.
/anonpass2:<*contraseña*>	(Opcional) Si la base de datos de origen está anonimizada con dos claves de anonimización, escriba la contraseña de anonimización secundaria para descifrar los datos exportados.

Ejemplo

```
EsmDlibM.exe /exportToSQL /server:192.168.11.11
/database:EventsDatabase /dbauth:SQL /username:sa /password:p@ss
/table:EventsTable /anonpass1:pa$$
```

16.3 Usar DLibAdm.exe

Se usa DLibAdm.exe para ejecutar operaciones administrativas en los servidores de bases de datos DLib instalados en la red.

Para utilizar DLibAdm.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.

2. Haga clic en **Ctrl + Shift + Enter** para ejecutar **CMD** como administrador.

3. Cambie el directorio activo a la carpeta de instalación del servidor de bases de datos DLib. Escriba (ejemplo):

```
CD C:\Program Files\GFI\Database Server 2.0
```

Presione la tecla **Enter**.

4. Escriba **DLibAdm.exe** seguido por las funciones que se describen a continuación:

» /decryptDatabase

» /encryptDatabase

- /displayAllDLib
- /copyMoveDLib

16.3.1 /decryptDatabase

Esta función le permite descifrar una base de datos DLib cifrada. Se admiten los siguientes parámetros:

Tabla 113: Parámetros /decryptDatabase

Parámetro	Descripción
/dbPath:<*ruta*>	Especifique la ruta a la base de datos que desea descifrar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/dbName:<*nombre*>	Especifique el nombre de la base de datos que desea descifrar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	Especifique la contraseña que se utiliza para descifrar la base de datos.

Ejemplo

```
DLibAdm.exe /decryptDatabase /dbPath:"C:\Program Files\GFI\Database
Server 2.0" /dbName:EventsDatabase /password:p@ss
```

16.3.2 /encryptDatabase

Esta función le permite cifrar una base de datos especificada. Se admiten los siguientes parámetros:

Tabla 114: Parámetros /encryptDatabase

Parámetro	Descripción
/dbPath:<*ruta*>	Especifique la ruta a la base de datos que desea cifrar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/dbName:<*nombre*>	Especifique el nombre de la base de datos que desea cifrar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/password:<*contraseña*>	Especifique la contraseña que se utiliza para cifrar la base de datos.

Ejemplo

```
DLibAdm.exe /encryptDatabase /dbPath:"C:\Program Files\GFI\Database
Server 2.0" /dbName:EventsDatabase /password:p@ss
```

16.3.3 /displayAllDLib

Esta función le permite enumerar todos los servidores de bases de datos DLib válidos que se ejecutan en una carpeta especificada. Se admite el siguiente parámetro:

Tabla 115: Parámetros /displayAllDLib

Parámetro	Descripción
/path:<*ruta*>	Especifique la ruta de la carpeta en la que desea buscar los servidores de bases de datos DLib válidos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
DLibAdm.exe /displayAllDLib /path:"C:\Program Files\GFI\Database
Server 2.0"
```

16.3.4 /copyMoveDLib

Esta función le permite copiar o mover una base de datos DLlib a una ubicación determinada. Se admiten los siguientes parámetros:

Tabla 116: /copyMoveDLib

Parámetro	Descripción
/sourcePath:<*sourcePath*>	Especifique la ruta a la base de datos de origen (la base de datos que desea mover o copiar). **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/destinationPath:<*destinationPath*>	Especifique la ruta a la carpeta de destino. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/copyMove:<*copy*|*move*>	Especifique la acción que desea llevar a cabo en la base de datos. Valores admitidos: » copiar » mover
/dbName:<*dbName*>	Especifique el nombre de la base de datos que desea copiar o mover. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
DLibAdm.exe /copyMoveDLib /sourcePath:"C:\Program Files\GFI\Database
Server 2.0" /destinationPath:C:\EventsDatabases /copyMove:move
/dbName:EventsDatabase
```

16.4 Usar EsmReport.exe

EsmReport.exe le permite generar informes en el producto, como informes de configuración y actividades de tareas.

Para utilizar EsmReport.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.
2. Haga clic en **Ctrl + Shift + Enter** para ejecutar CMD con privilegios elevados.
3. Cambie el directorio al directorio de instalación de GFI EventsManager. Ejemplo:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Escriba **EsmReport.exe** seguido de cualquiera de las siguientes funciones:

- Generar informes de configuración
- Generar informes de estado
- Generar informes de eventos

16.4.1 Generar informes de configuración

Esta función le permite generar informes de configuración de un único origen de eventos o de un grupo de orígenes de eventos. Se admiten los siguientes parámetros:

Tabla 117: Parámetros de los informes de configuración

Parámetro	Descripción
/type:<*configuration*|*status*|*events*>	Especifique el tipo de informe que desea generar. Se admiten los siguientes valores: » configuración » status (para estado) » events (para eventos) Escriba **/type:configuration** para generar un informe de configuración.
/target:<*ruta*>	Especifique la ruta de acceso a la carpeta donde se guarda el informe generado. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/format:<*html*|*csv*>	Especifique el formato del informe. Se admiten los siguientes valores: » html » csv
/source:<*name*>	Especifique el nombre del origen de los eventos. Utilice este parámetro para generar un informe de configuración de un único origen de eventos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/group:<*name*>	Especifique el nombre del grupo de orígenes de los eventos. Utilice este parámetro para generar un informe de configuración de un grupo de orígenes de eventos. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
EsmReport.exe /type:configuration /target:C:\ReportsFolder
/format:html /group:"Domain Controllers"
```

16.4.2 Generar informes de estado

Esta función le permite generar informes de estado de GFI EventsManager. Se admiten los siguientes parámetros:

Tabla 118: Parámetros de informes de estado

Parámetro	Descripción
/type:<*configuration*|*status*|*events*>	Especifique el tipo de informe que desea generar. Se admiten los siguientes valores: » configuración » status (para estado) » events (para eventos) Escriba **/type:status** para generar un informe de estado.
/subtype:<*messages*|*stats*>	Especifique el tipo de informe de estado que desea generar. Se admiten los siguientes valores: » **messages**: cuando se especifica este tipo, se pueden utilizar los siguientes parámetros: • **/period:<*current*|*date*>**: escriba **current** para generar un informe que contenga los mensajes generados en el mismo día. O bien, escriba una fecha para generar un informe de estado que contenga los mensajes generados en la fecha especificada. » **stats**: cuando se especifica stats como un subtipo, se pueden utilizar los siguientes parámetros: • **/format:<*html*|*csv*>**: especifique el formato del informe. Los valores admitidos son **HTML** y **CSV**. • **/period:<*"all time"*|*date*>** : especifique el período de tiempo en el que se basa el informe. Los valores admitidos incluyen "**all time**" para todos los períodos, o bien una fecha específica. • **/options:<*"error messages"*|*"only with issues"*>**: especifique el tipo de estadísticas que desea generar. Los valores admitidos son "**error messages**" y "**only with issues**", para mensajes de error y solamente con problemas, respectivamente. • **/target:<*ruta*>**: especifique la ruta de acceso a la carpeta donde se guarda el informe. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo de mensajes

```
EsmReport.exe /type:status /subtype:messages /period:"current date"
```

Ejemplo de estadísticas

```
EsmReport.exe /type:status /subtype:stats /format:html
/period:20130111 /options:"error messages" /target:C:\StatsReports
```

16.4.3 Generar informes de eventos

Esta función le permite generar informes de eventos. Se admiten los siguientes parámetros:

Tabla 119: Parámetros de informes de eventos

Parámetro	Descripción
/type:<*configuration*|*status*|*events*>	Especifique el tipo de informe que desea generar. Se admiten los siguientes valores: » configuración » status (para estado) » events (para eventos) Escriba **/type:events** para generar un informe de eventos.
/repname:<*fullReportName*>	Especifique un nombre para el informe generado. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/repid:<*reportID*>	Especifique un ID único para el informe generado. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/target<*ruta*>	Especifique la ruta de acceso a la carpeta donde se guarda el informe. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/format:<*html*|*csv*>	Especifique el formato del informe. Se admiten los siguientes valores: » html » csv
/datefrom:<*startDate*>	Especifique la fecha de inicio del período de tiempo del que desea obtener un informe.
/dateto:<*endDate*>	Especifique la fecha de finalización del período de tiempo del que desea obtener el informe.
/scheduled	Especifique este parámetro para generar el informe basado en los parámetros de programación que se configuraron en la Consola de administración.

Ejemplo

```
EsmReport.exe /type:events /repname:"New Events Report" /repid:11
/target:C:\ReportsFolder /format:html /datefrom:20121201
/dateto:20130111
```

16.4.4 Usar ImportSettings.exe

Importsettings.exe le permite importar la configuración de una carpeta de datos o de un archivo de configuración que se exportó desde otra instancia de GFI EventsManager. Utilice esta herramienta para obtener copias de seguridad de los parámetros de configuración de la Consola de administración.

Para utilizar ImportSettings.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.
2. Haga clic en **Ctrl + Shift + Enter** para ejecutar CMD con privilegios elevados.
3. Cambie el directorio al directorio de instalación de GFI EventsManager. Ejemplo:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Escriba **ImportSettings.exe** seguido de los parámetros que se describen a continuación:

Tabla 120: CMD: Parámetros de ImportSettings.exe

Parámetro	Descripción
/operation:<*operación*>	Especifique la operación que desea realizar. Se admiten los siguientes valores: » importFile » importFolder
/destination: <*carpeta*>	Especifique la carpeta de destino donde se importa la configuración. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/sourceFile: <*nombre de archivo*>	Especifique el nombre del archivo que contiene las configuraciones exportadas. Utilice este parámetro para definir el nombre del archivo cuando se ejecuta una operación **importFile**. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/sourceFolder: <*nombre de la carpeta*>	Especifique el nombre de la carpeta que contiene las configuraciones exportadas. Utilice este parámetro para definir el nombre de la carpeta cuando se ejecuta una operación **importFolder** **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/id:<*EsmInstanceID*>	Solamente se puede utilizar este parámetro cuando desea cambiar el ID de la instancia de GFI EventsManager. Si no se especifica un valor, se conserva el mismo ID. Si no utiliza este parámetro, son obligatorios los parámetros **/operation**, **/destination**, **/sourceFile** o **/sourceFolder**.

Ejemplo

```
ImportSettings.exe /operation:importFile
/destination:C:\NewDestination /sourceFile:C:\ExportedSettings
```

O BIEN

```
ImportSettings.exe /id:newInstanceID
```

16.4.5 Usar ExportSettings.exe

ExportSettings.exe le permite exportar los parámetros de configuración de GFI EventsManager a un archivo de configuración.

Para utilizar ExportSettings.exe:

1. Haga clic en **Start > Run** y escriba **CMD**.
2. Haga clic en **Ctrl + Shift + Enter** para ejecutar CMD con privilegios elevados.
3. Cambie el directorio al directorio de instalación de GFI EventsManager. Ejemplo:

```
CD <C:\Program Files\GFI\EventsManager>
```

4. Escriba **ExportSettings.exe** seguido de los parámetros que se describen a continuación:

Tabla 121: CMD: Parámetros ExportSettings.exe

Parámetro	Descripción
/destination: ***<nombre de archivo>***	Especifique una ruta de carpeta válida que incluya el nombre del archivo donde se exportan los parámetros. A menos que se especifique lo contrario, **.esmbkp** se anexa como una extensión al nombre de archivo. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).
/folder:<*carpeta*>	Este parámetro se utiliza para indicar a la herramienta que exporte los parámetros desde un lugar distinto a la carpeta de datos predeterminada. Especifique la ruta a la carpeta que contenga los parámetros de datos de GFI EventsManager que desea exportar. **Nota** Los parámetros que contienen espacios deben escribirse entre comillas dobles (“).

Ejemplo

```
ExportSettings.exe /destination:C:\NewDestination
```

17 Varios

En este capítulo, se proporciona información relacionada con la configuración de los componentes de terceros necesarios para las operaciones de auditoría de GFI EventsManager. Más información sobre cómo configurar y ejecutar acciones de GFI EventsManager a través de las herramientas de línea de comandos proporcionadas.

Temas de este capítulo:

17.1 Activar permisos de orígenes de eventos manualmente 339

17.2 Activar permisos de orígenes de eventos automáticamente 347

17.3 Desactivar Control de cuentas de usuario (UAC) 352

17.1 Activar permisos de orígenes de eventos manualmente

En esta sección, se describe cómo configurar los permisos requeridos por GFI EventsManager para auditar sistemas y procesar los eventos necesarios. Este proceso se tiene que llevar a cabo en cada máquina que se desea analizar.

Esta sección contiene información acerca de:

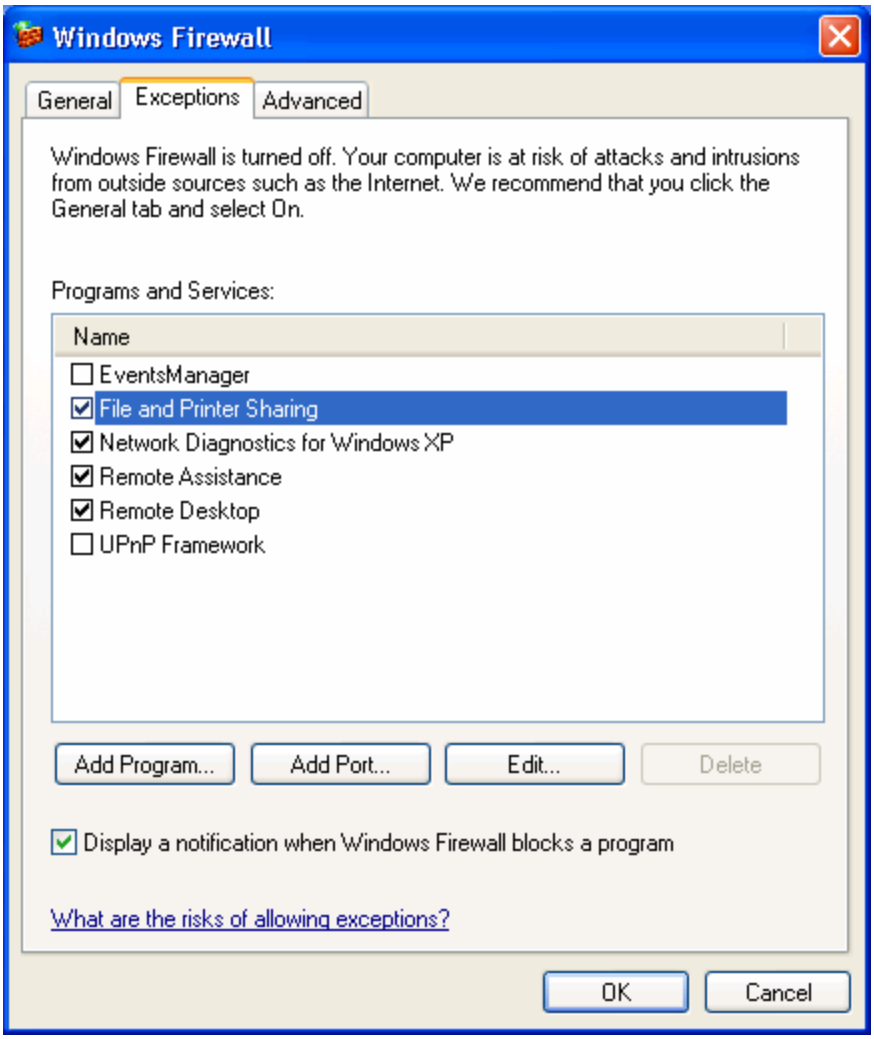
- Activar permisos en Microsoft® Windows® XP
- Activar permisos en Microsoft® Windows® Vista
- Activar permisos en Microsoft® Windows® 7
- Activar permisos en Microsoft® Windows® Server 2003
- Activar permisos en Microsoft® Windows® Server 2008 (incluido R2)

> **Nota**
>
> En un entorno de directorio activo, los permisos se pueden configurar de forma automática a través de Group Policy Object (GPO). Para obtener más información, consulte Activar permisos de orígenes de eventos automáticamente.

17.1.1 Activar permisos en Microsoft® Windows® XP

Para activar permisos de orígenes de eventos de Microsoft® Windows®:

1. Haga clic en la ficha **Start > Control Panel > Windows Firewall > Exceptions**.



Captura de pantalla 277: Reglas del firewall en Microsoft® Windows® XP

2. En la lista **Programs and Services**, active **File and Printer Sharing**.

3. Haga clic en **Aceptar**.

17.1.2 Activar permisos en Microsoft® Windows® Vista

Para activar permisos en máquinas que ejecutan Microsoft® Windows® Vista:

- Paso 1: Active los permisos de firewall
- Paso 2: Active las características adicionales de auditoría

Paso 1: Activar permisos de firewall

1. Haga clic en **Start > Control Panel > Security** y haga clic en **Allow a program through Windows Firewall** en el panel izquierdo.

2. Seleccione la ficha **Exceptions** y, en la lista **Allowed programs and features**, active las siguientes reglas:

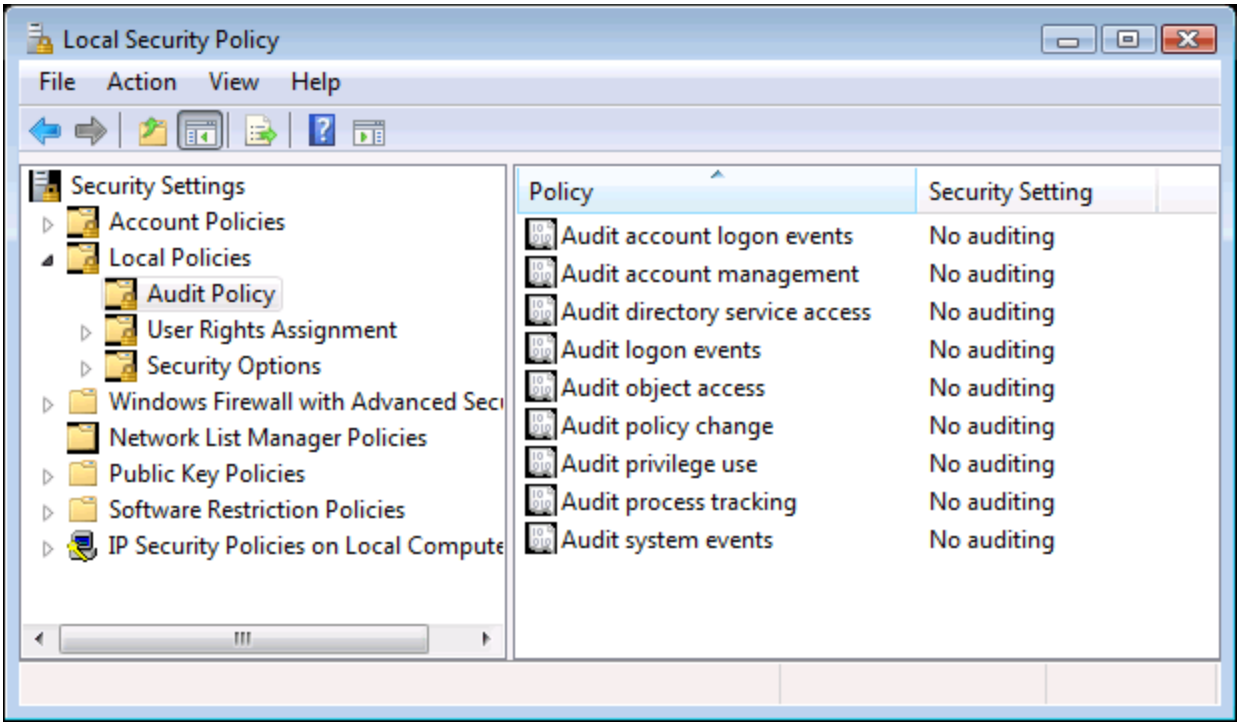
- Administración remota de registros de eventos
- Uso compartido de archivos e impresoras
- Detección de redes

3. Haga clic en **Aplicar**.

Paso 2: Activar características adicionales de auditoría

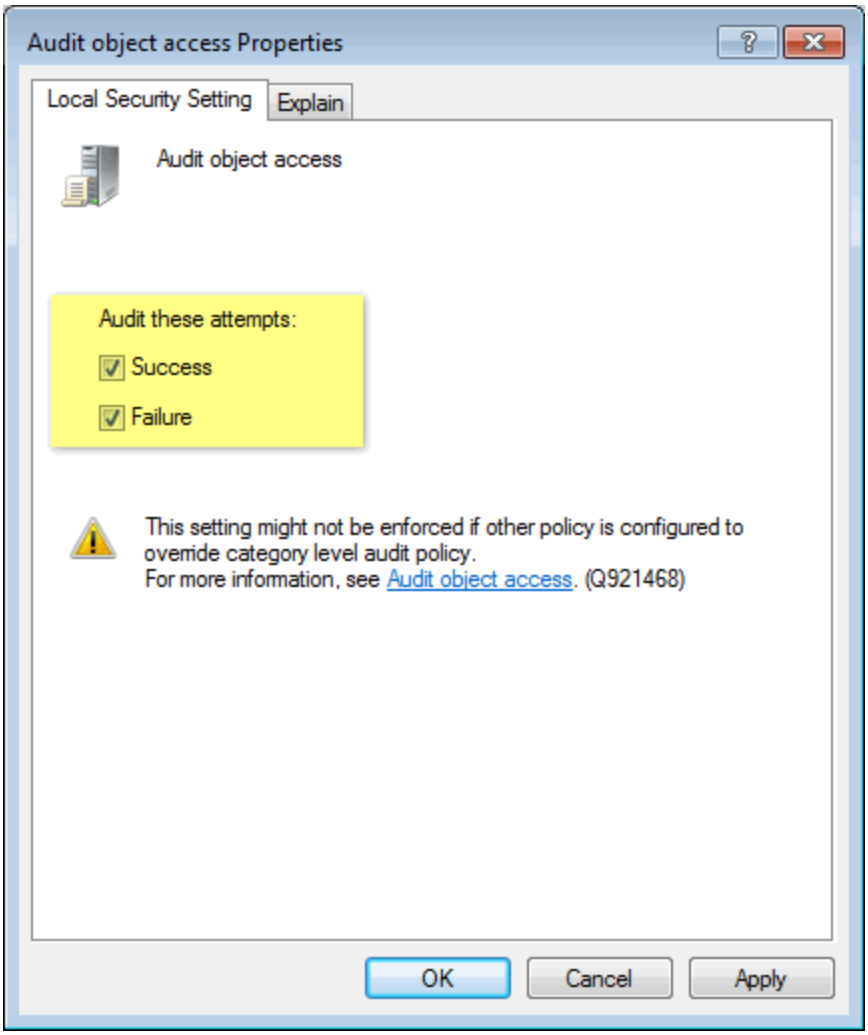
1. Haga clic en **Start > Run** y escriba **secpol.msc**. Presione la tecla **Enter**.

2. En el nodo **Security Settings**, amplíe **Local Policies > Audit Policy**.



Captura de pantalla 278: Ventana de política de seguridad local

3. En el panel derecho, haga doble clic en **Audit object access**.



Captura de pantalla 279: Auditar propiedades de acceso a objetos

4. En **Audit object access Properties**, seleccione **Success** y **Failure** y haga clic en **OK**.
5. En el panel derecho, haga doble clic en **Audit Process tracking**.
6. En **Audit object access Properties**, seleccione **Success** y **Failure** y haga clic en **OK**.
7. En el panel derecho, haga doble clic en **Audit account management**.
8. En **Audit object access Properties**, seleccione **Success** y **Failure** y haga clic en **OK**.
9. En el panel derecho, haga doble clic en **Audit system events**.
10. En **Audit process tracking Properties**, seleccione **Success** y **Failure** y haga clic en **OK**.
11. Cierre la ventana Local Security Policy.

17.1.3 Activar permisos en Microsoft® Windows® 7

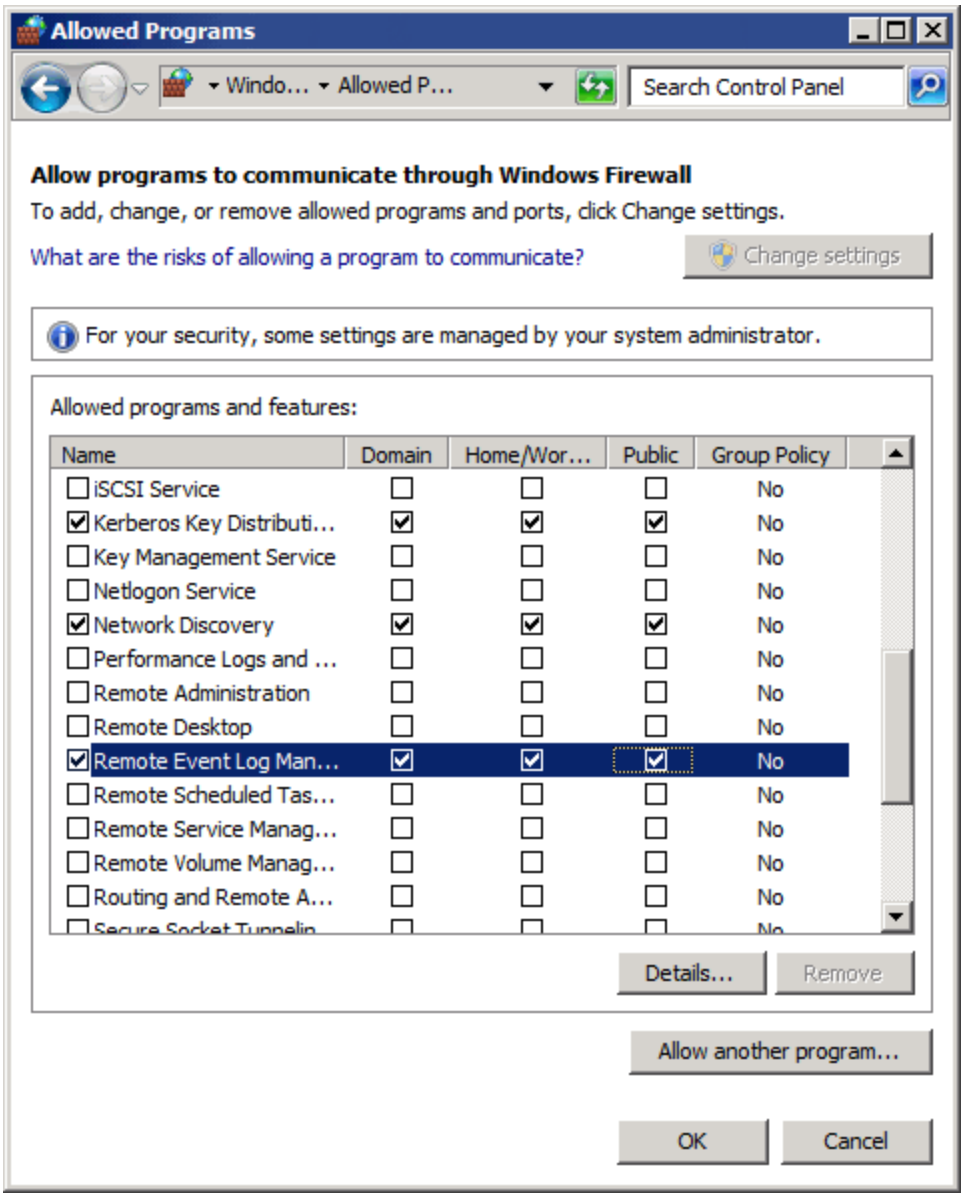
Para activar permisos en máquinas con Microsoft® Windows® 7:

- Paso 1: Active los permisos de firewall
- Paso 2: Active las características adicionales de auditoría

Paso 1: Activar permisos de firewall

Para activar manualmente las reglas del firewall en Microsoft® Windows® 7:

1. Haga clic en **Start > Control Panel > System and Security** y haga clic en **Allow a program through Windows Firewall** en la categoría Windows Firewall.



Captura de pantalla 280: Programas admitidos en Microsoft® Windows® Vista o una versión posterior

2. En la lista **Allowed programs and features**, active las siguientes reglas:

- Administración remota de registros de eventos
- Uso compartido de archivos e impresoras
- Detección de redes

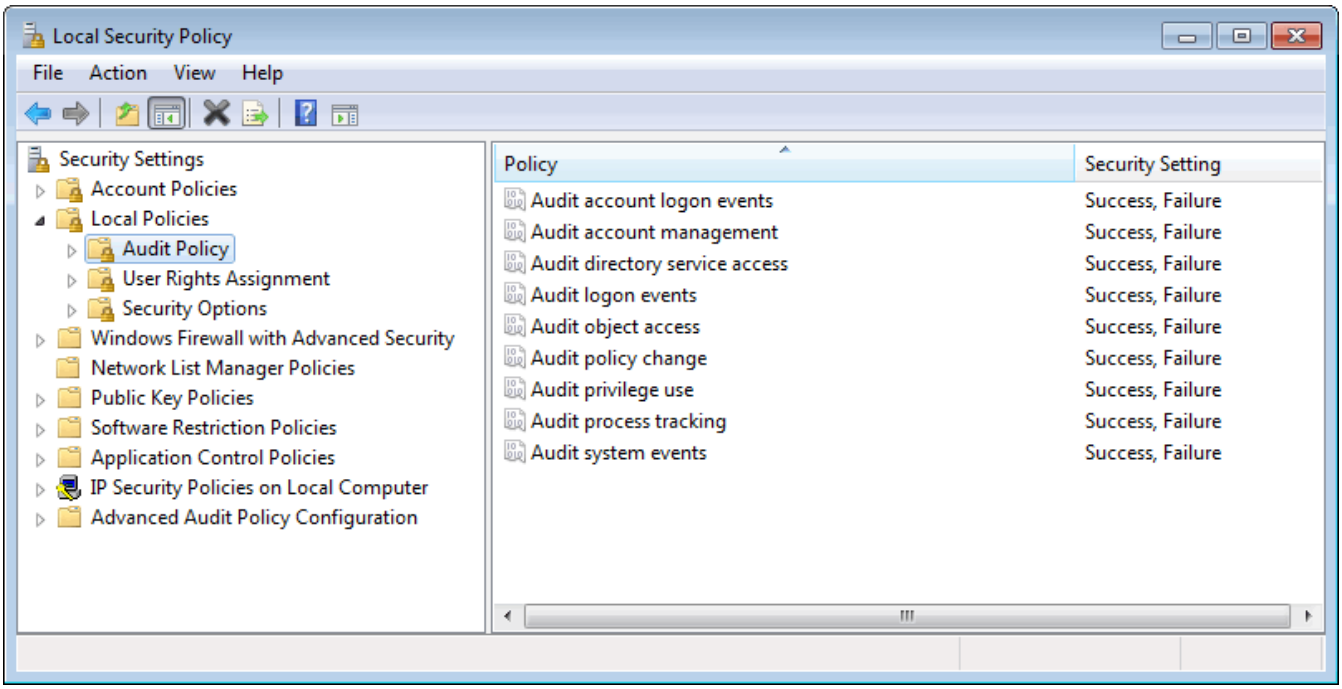
3. Seleccione **Domain**, **Private** y **Public** para cada regla mencionada anteriormente.

4. Haga clic en **Aceptar**.

Paso 2: Activar características adicionales de auditoría

1. Haga clic en **Start > Run** y escriba **secpol.msc**. Presione la tecla **Enter**.

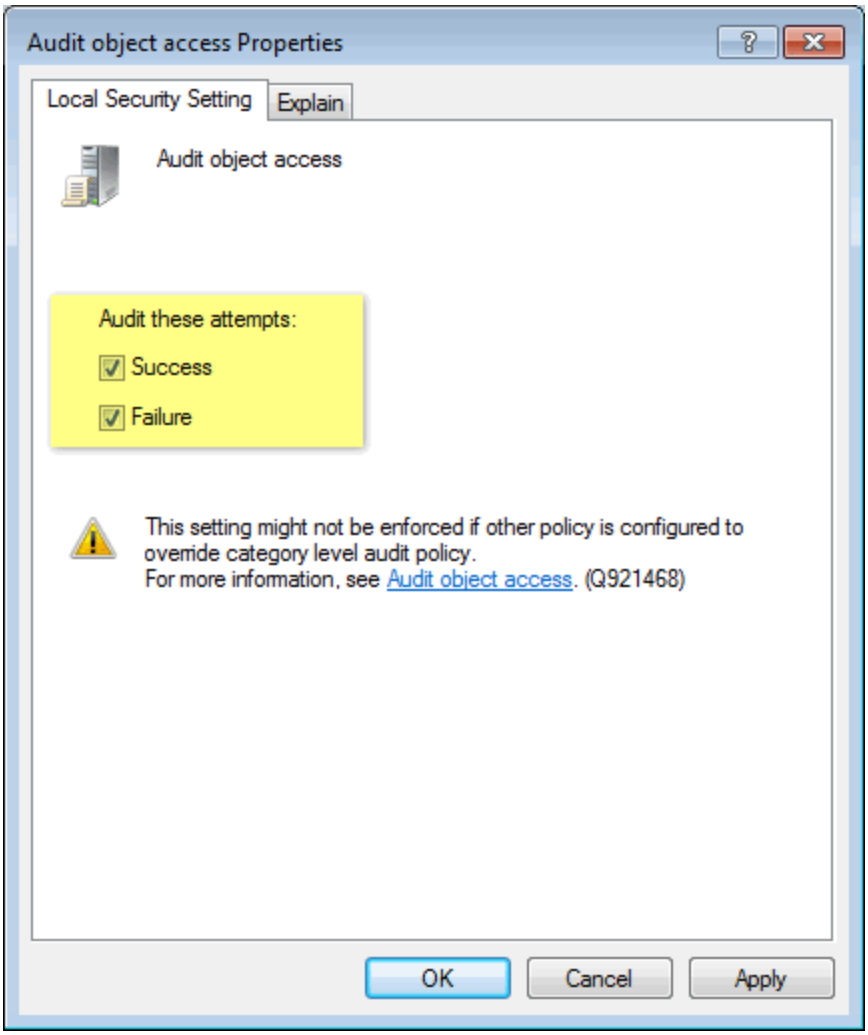
2. En el nodo **Security Settings**, amplíe **Local Policies > Audit Policy**.



Captura de pantalla 281: Ventana de política de seguridad local

3. En el panel derecho, haga doble clic en **Audit object access**.

4. En **Audit object access Properties**, seleccione **Success** y **Failure**. Haga clic en **Aceptar**.



Captura de pantalla 282: Auditar propiedades de acceso a objetos

5. En el panel derecho, haga doble clic en **Audit Process tracking**.

6. En **Audit process tracking Properties**, seleccione **Success** y **Failure**. Haga clic en **Aceptar**.

7. En **Audit process tracking Properties**, seleccione **Success** y **Failure**. Haga clic en **Aceptar**.

8. En el panel derecho, haga doble clic en **Audit account management**.

9. En **Audit process tracking Properties**, seleccione **Success** y **Failure**. Haga clic en **Aceptar**.

10. En el panel derecho, haga doble clic en **Audit system events**.

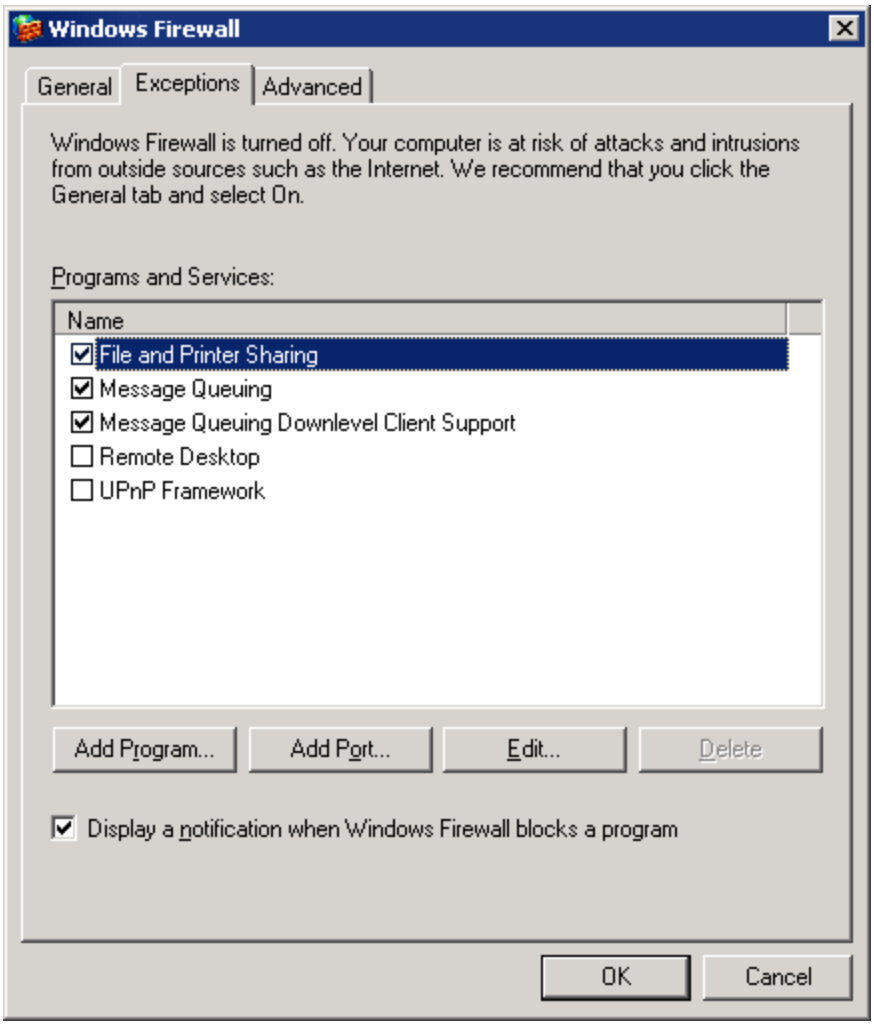
11. En **Audit process tracking Properties**, seleccione **Success** y **Failure**. Haga clic en **Aceptar**.

12. Cierre la ventana Local Security Policy.

17.1.4 Activar permisos en Microsoft® Windows® Server 2003

Para activar manualmente las reglas del firewall en Microsoft® Windows® Server 2003:

1. Haga clic en **Start > Control Panel > Windows Firewall** y seleccione la ficha **Exceptions**.



Captura de pantalla 283: Activar reglas del firewall en Microsoft® Windows® Server 2003

2. En la lista **Programs and Services**, active **File and Printer Sharing**.

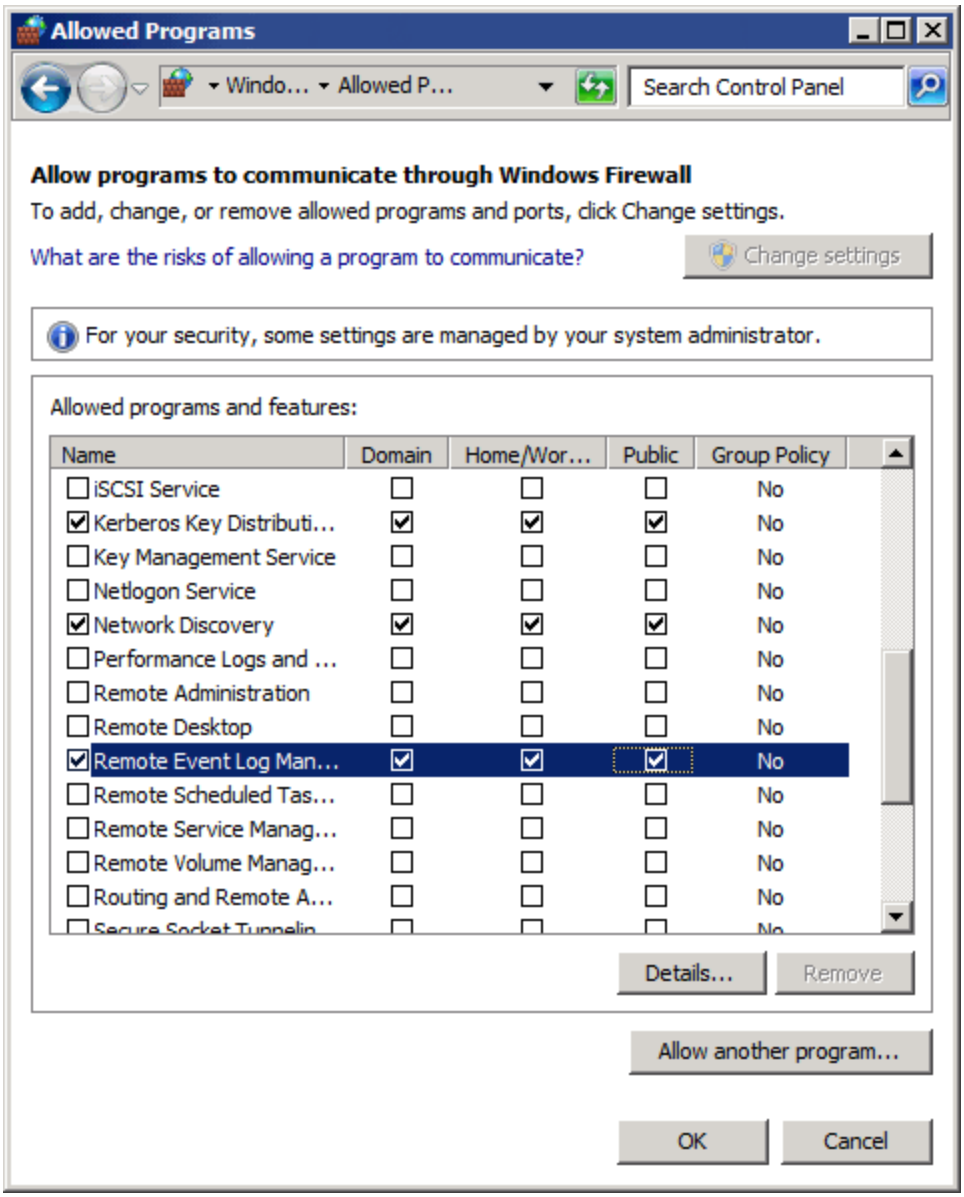
3. Haga clic en **Aceptar**.

17.1.5 Activar permisos en Microsoft® Windows® Server 2008 (incluido R2)

1. Haga clic en **Start > Control Panel > Security** y haga clic en **Allow a program through Windows Firewall** en la categoría **Windows Firewall**.

2. En la lista de programas, active:

- Uso compartido de archivos e impresoras
- Detección de redes
- Administración remota de registros de eventos



Captura de pantalla 284: Reglas del firewall en Microsoft®Windows® Server 2008

3. Haga clic en **Aceptar**.

> **Nota**
>
> En Windows® Server 2008 R2, asegúrese de seleccionar **Domain**, **Private** y **Public** para cada regla mencionada anteriormente.

17.2 Activar permisos de orígenes de eventos automáticamente

Esta sección contiene información acerca de:

- Activar permisos en Windows® Server 2003 a través de GPO
- Activar permisos en Windows® Server 2008 a través de GPO

17.2.1 Activar permisos en Windows® Server 2003 a través de GPO

Para abrir permisos activados en los clientes de todos los dominios que utilizan el controlador de dominio de Microsoft® Windows® Server 2003:

1. Haga clic en **Start > Run** y escriba **mmc**. Presione la tecla **Enter**.

2. Haga clic en **File > Add/Remove Snap-in** y haga clic en **Add**.

3. Busque y seleccione **Group Policy Object Editor** y haga clic en **Add**.

4. Haga clic en **Browse**, seleccione **Default Domain Policy** y haga clic en **OK**.

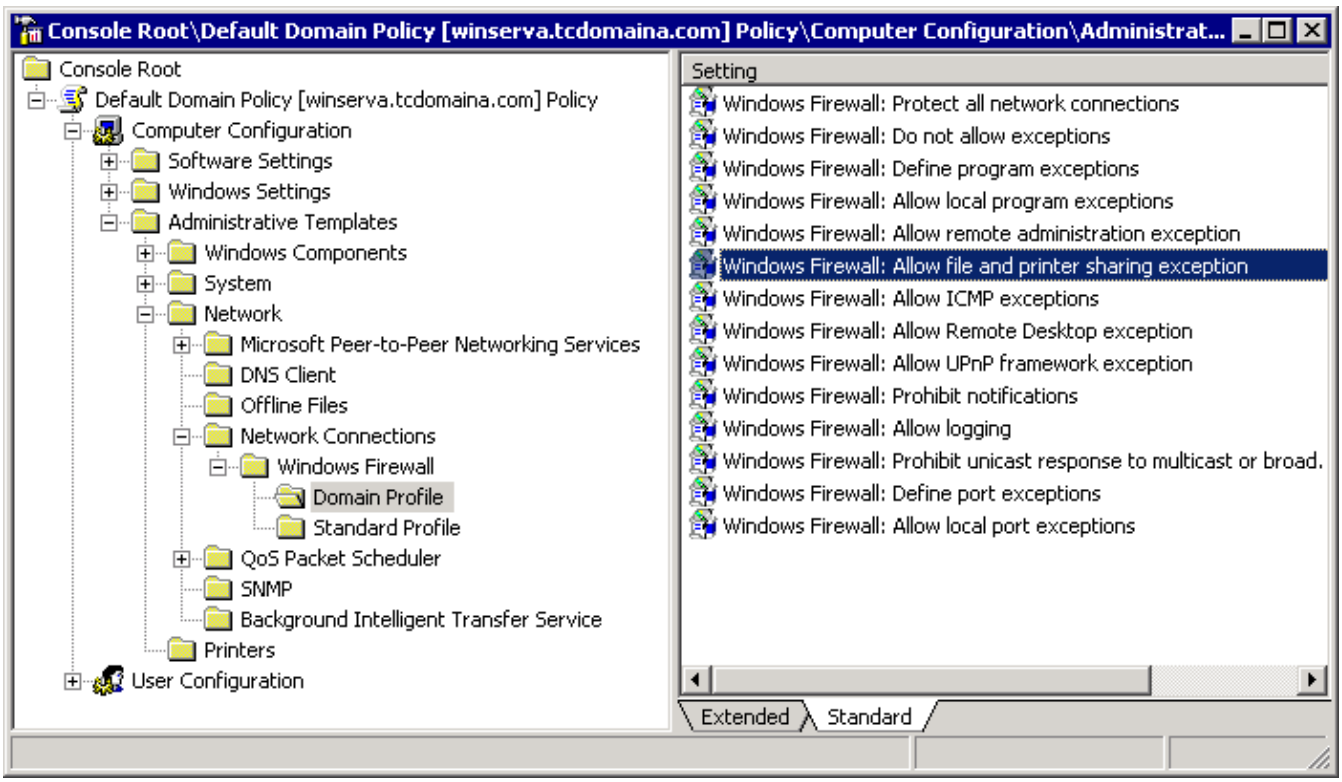
5. Haga clic en **Finish** para finalizar.

6. Seleccione **Group Policy Object Editor** de nuevo y haga clic en **Add**.

7. Haga clic en **Browse**, haga doble clic en la carpeta **Domain Controllers** y seleccione **Default Domain Controllers Policy**. Haga clic en **Aceptar**.

8. Haga clic en **Finish** y **Close**.

9. En **Console Root**, expanda **Default Domain Policy > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.



Captura de pantalla 285: Consola de política de dominio en Microsoft® Windows® Server 2003

10. En la lista **Setting**, haga clic en **Windows Firewall: Allow file and printer sharing exception** y seleccione **Properties**.

11. En la ficha **Settings**, seleccione **Enabled** y haga clic en **OK**.

12. Repita los Pasos 9 a 11 para **Default Domain Controllers Policy**.

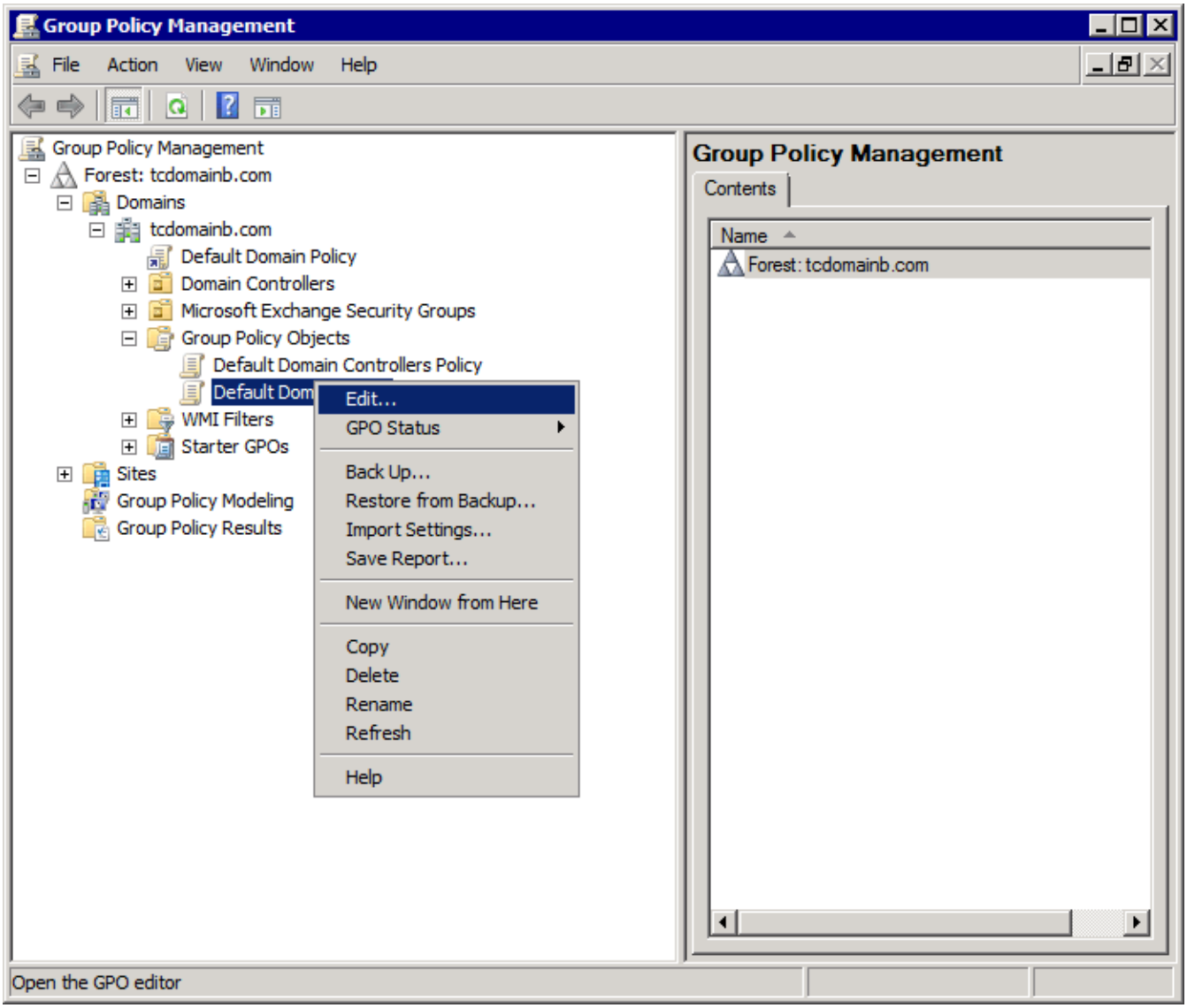
13. Haga clic en **File > Save** para guardar la consola de administración. La política del grupo entra en vigor la próxima vez que se reinicie cada equipo.

17.2.2 Activar permisos en Windows® Server 2008 a través de GPO

Para activar permisos en los clientes de todos los dominios:

1. Haga clic en **Start > Administrative Tools > Group Policy Management**.

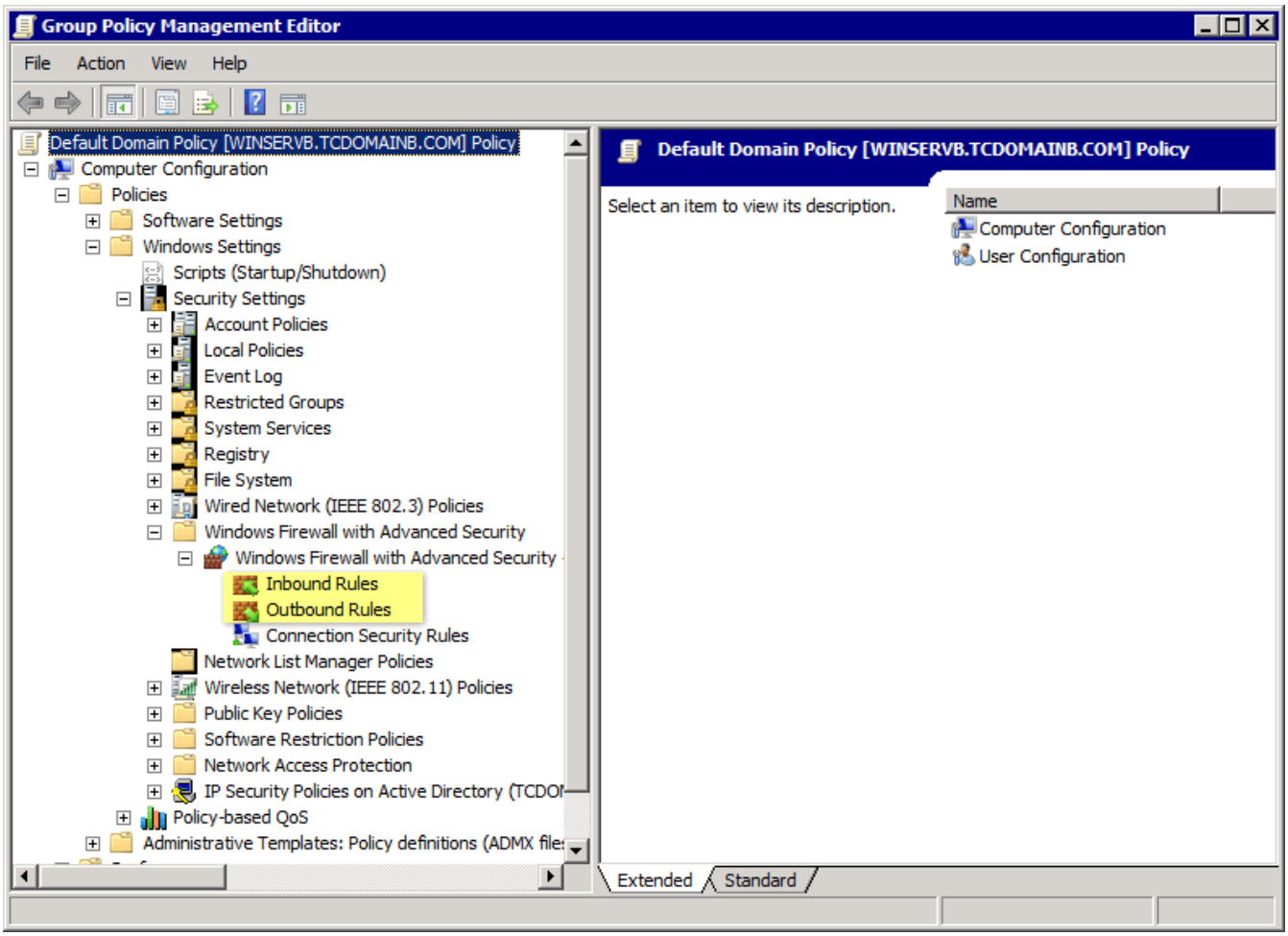
2. Expanda **Group Policy Management > Forest > Domains > <*Nombre de dominio*> > Group Policy Objects**.



Captura de pantalla 286: Administración de políticas de grupo en Microsoft® Windows® Server 2008 R2

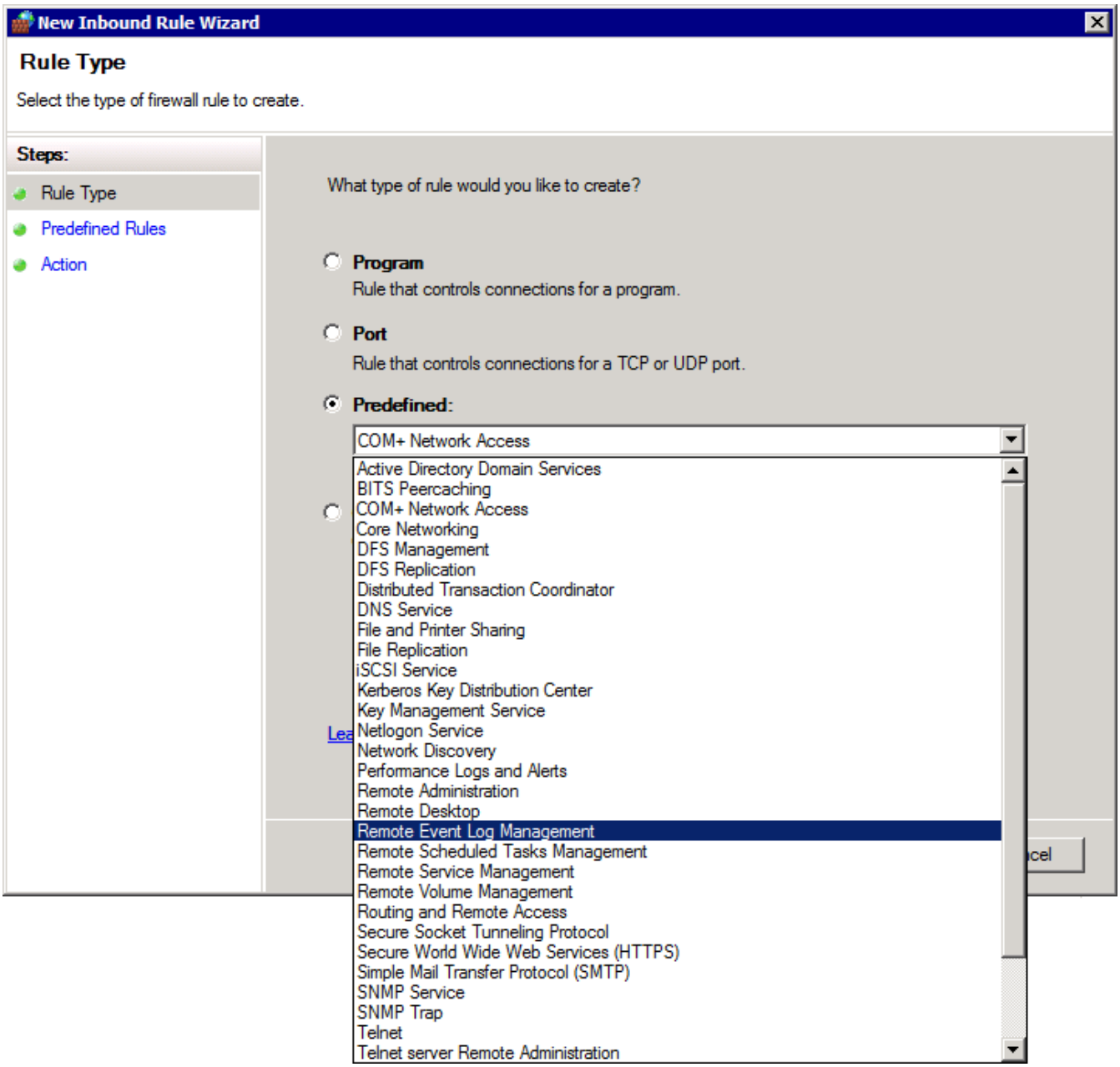
3. Haga clic con el botón secundario en **Default Domain Policy** y seleccione **Edit**.

4. Expanda **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, haga clic con el botón secundario en **Inbound Rules** y seleccione **New Rule…**.



Captura de pantalla 287: Editor de administración de políticas de grupo

5. En el asistente **New Inbound Rule**, seleccione **Predefined** y seleccione **File and Printer Sharing**.



Captura de pantalla 288: Reglas predefinidas

6. Haga clic en **Next**.

7. Seleccione todas las reglas y haga clic en **Next**.

8. Seleccione **Allow the connection** y haga clic en **Finish**.

9. Repita los Pasos 5 a 8 para cada una de las siguientes reglas:

» Administración remota de registros de eventos

» Detección de redes

10. En **Group Policy Management Editor**, expanda **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, haga clic con el botón secundario en **Outbound Rules** y seleccione **New Rule...**.

11. Repita los Pasos 5 al 9, pero en el Paso 9 active solamente **Network discovery**.

12. Cierre **Group Policy Management Editor**.

13. En **Group Policy Management**, expanda **Group Policy Management > Forest > Domains > <*Nombre de dominio*> > Default Domain Controllers Policy**.

14. Repita los Pasos 4 a 13.

15. Haga clic en **File > Save** para guardar la consola de administración. La política del grupo entra en vigor la próxima vez que se reinicie cada equipo.

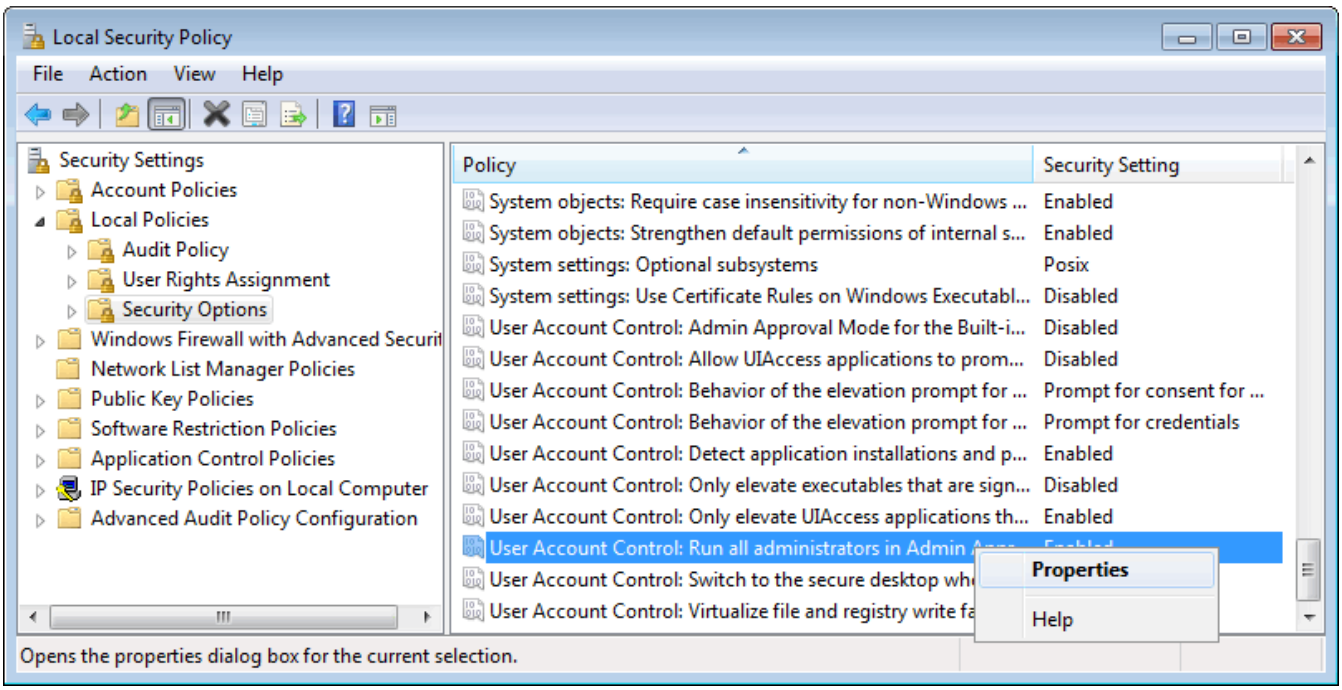
17.3 Desactivar Control de cuentas de usuario (UAC)

Cuando GFI EventsManager se configura para recopilar eventos utilizando una cuenta local, los equipos de destino deben tener desactivado el **Control de cuenta de usuario (UAC)**. Para desactivar el UAC en máquinas con Microsoft® Windows® Vista o una versión posterior:

1. Haga clic en **Start > Run**, ingrese **secpol.msc** y presione **Enter**.

2. En **Security Settings**, expanda **Local Policies** y haga clic en **Security Options**.

3. Haga clic con el botón secundario en **User Account Control: Run all administrators in Admin Approval Mode** y seleccione **Properties**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Securit
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
System objects: Require case insensitivity for non-Windows ... Enabled
System objects: Strengthen default permissions of internal s... Enabled
System settings: Optional subsystems Posix
System settings: Use Certificate Rules on Windows Executabl... Disabled
User Account Control: Admin Approval Mode for the Built-i... Disabled
User Account Control: Allow UIAccess applications to prom... Disabled
User Account Control: Behavior of the elevation prompt for ... Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ... Prompt for credentials
User Account Control: Detect application installations and p... Enabled
User Account Control: Only elevate executables that are sign... Disabled
User Account Control: Only elevate UIAccess applications th... Enabled
User Account Control: Run all administrators in Admin
User Account Control: Switch to the secure desktop wh
User Account Control: Virtualize file and registry write fa
Properties
Help
Opens the properties dialog box for the current selection.

Captura de pantalla 289: Desactivar UAC

4. En la ficha **Local Security Settings**, seleccione **Enabled** y haga clic en **OK**.

5. Cierre la ventana Local Security Policy.

18 Solución de problemas

Utilice la información de las secciones siguientes para resolver los problemas detectados en GFI EventsManager:

- Documentación
- GFI SkyNet
- Solicitar soporte técnico
- Foro en la red
- Asistente para el solucionador de problemas

18.1 Documentación

Si este manual no cumple sus expectativas o si cree que esta documentación se puede mejorar, indíquenoslo enviando un correo electrónico a: documentation@gfi.com.

18.2 GFI SkyNet

GFI mantiene un exhaustivo repositorio de su base de conocimientos, que incluye respuestas a los problemas más habituales. GFI SkyNet tiene siempre la lista más actualizada de preguntas y revisiones de soporte técnico. Si la información de esta guía no soluciona sus problemas, consulte GFI SkyNet; para ello, visite http://kb.gfi.com/.

18.3 Solicitar soporte técnico

Si ninguno de los recursos especificados anteriormente le permite solucionar los problemas, póngase en contacto con el equipo de Soporte técnico de GFI rellenando un formulario de solicitud de soporte técnico en línea, o bien de forma telefónica.

- **En línea**: Complete el formulario de solicitud de soporte técnico y siga las instrucciones detalladas que se indican en esta página para enviar su solicitud de soporte técnico en: http://support.gfi.com/supportrequestform.asp.
- **Teléfono**: Para obtener el número de teléfono de soporte técnico correspondiente a su región, visite: http://www.gfi.com/company/contact.htm.

> **Nota**
>
> Antes de ponerse en contacto con el Centro de soporte técnico, tenga su identificación de cliente a mano. Su ID de cliente es el número de cuenta en línea que se le asigna cuando registra por primera sus claves de licencia en el área de clientes de GFI en: http://customers.gfi.com.

Le responderemos en 24 horas, o antes, en función de su huso horario.

18.4 Foro en la red

El soporte técnico de usuario a usuario está disponible a través del foro web de GFI. Para acceder al foro web, visite: http://forums.gfi.com.

18.5 Asistente para el solucionador de problemas

Para usar el solucionador de problemas:

1. Vaya a la carpeta de instalación de GFI EventsManager.

2. Localice el archivo **Trouble.exe** y haga doble clic en él.

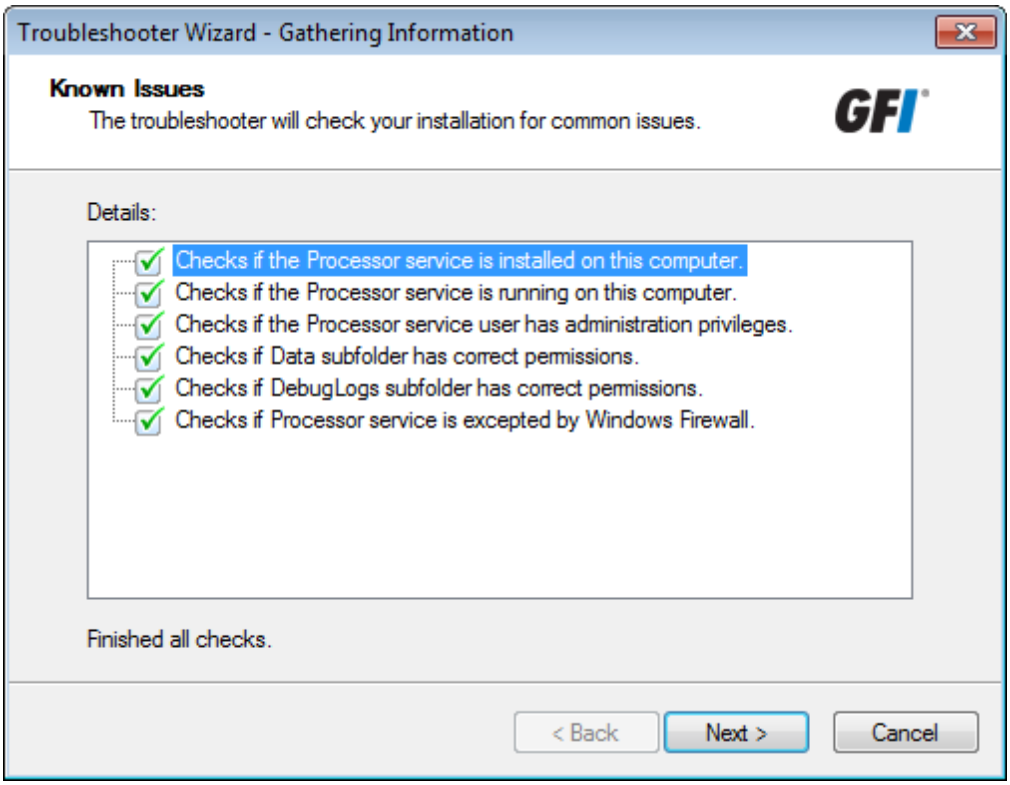
3. Haga clic en **Next** en la pantalla de bienvenida del asistente.

Troubleshooter Wizard - Gathering Information
Information Details
Please select the information to gather.
GFI
The troubleshooter should:
Automatically detect and fix known issues (Recommended)
Gather only application information and logs.
Note: Use this option when the problem is already located and only support files are needed.
< Back
Next >
Cancel

Captura de pantalla 290: Seleccione el modo de recopilación de datos

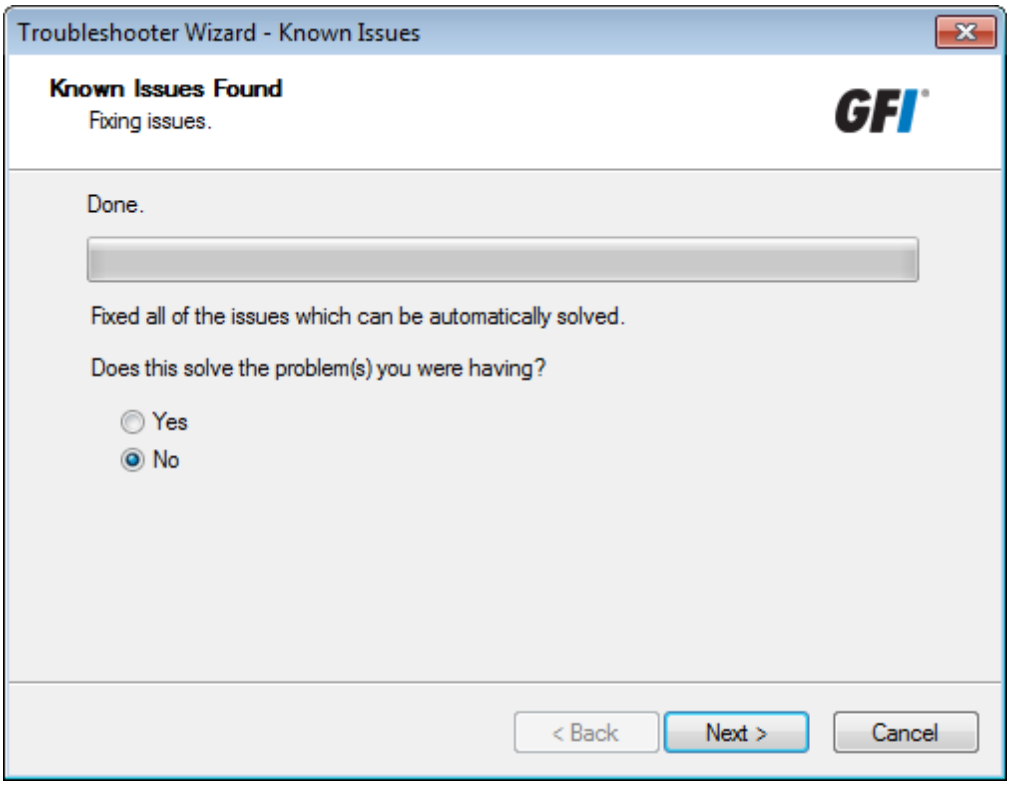
4. Seleccione cómo desea que el solucionador de problemas recopile la información. Seleccione una de las siguientes opciones:

- **Automatically detect and fix known issues**: esta opción permite que GFI EventsManager ejecute una serie de comprobaciones para determinar qué es incorrecto.
- **Gather only application information and logs**: especifique los detalles de contacto, la descripción del problema y la información del sistema para cargarlos y enviarlos a nuestro equipo de soporte. Si elige esta opción, omita los siguientes pasos y vaya directamente al Paso **9**.


Troubleshooter Wizard - Gathering Information
Known Issues
The troubleshooter will check your installation for common issues.
GFI
Details:
Checks if the Processor service is installed on this computer.
Checks if the Processor service is running on this computer.
Checks if the Processor service user has administration privileges.
Checks if Data subfolder has correct permissions.
Checks if DebugLogs subfolder has correct permissions.
Checks if Processor service is excepted by Windows Firewall.
Finished all checks.
< Back
Next >
Cancel

Captura de pantalla 291: Solucionador de problemas de comprobaciones automáticas

5. Espere hasta que el solucionador de problemas ejecute las comprobaciones necesarias y haga clic en **Next**.



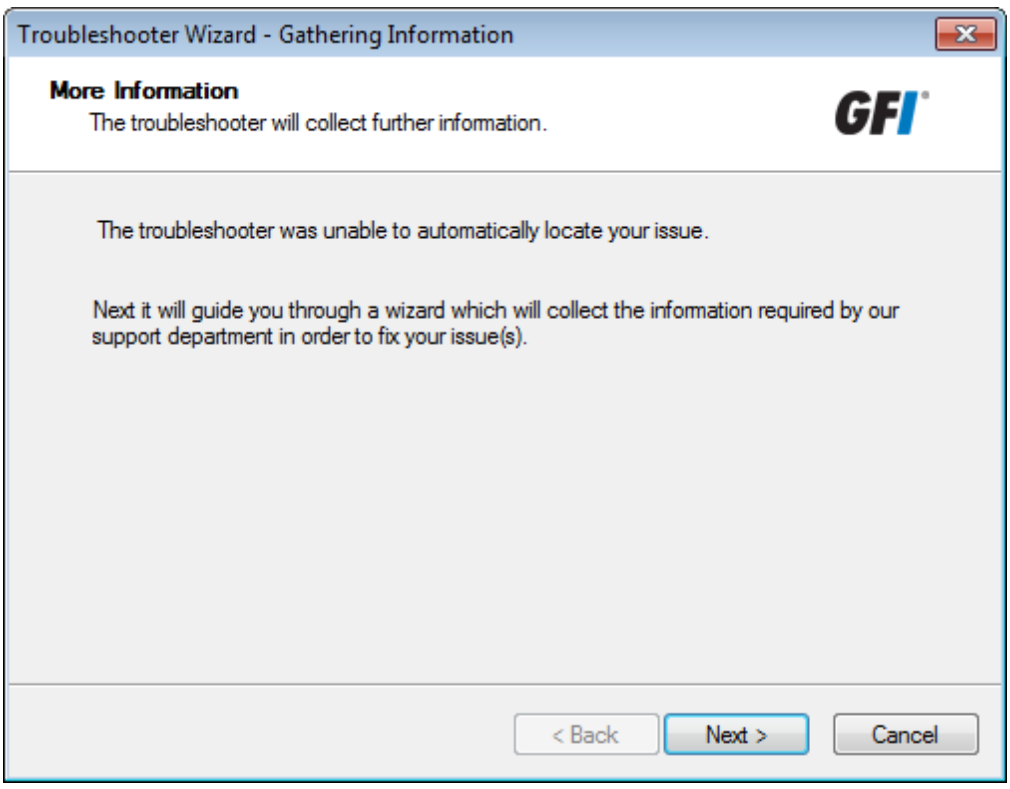
Captura de pantalla 292: Solucionador de problemas de corrección automática de problemas detectados

6. Espere hasta que el solucionador de problemas aplique las correcciones correspondientes a los problemas detectados durante la comprobación. Si esto no resuelve el problema, haga clic en **Yes** y **Finish**. Si el problema persiste, seleccione **No** y haga clic en **Next**.

Troubleshooter Wizard - Gathering Information
Search GFI Knowledge Base
Please fill in the appropriate information.
GFI
Enter search terms:
Cannot scan SQL Server sources
Search
Note: The search terms must be accurate. Entering more search terms will narrow your search and yield less results.
Search will be performed using the knowledge databases available at http://forums.gfi.com/ and http://kbase.gfi.com/.
Did the information found in the knowledge databases help you fix the issue(s)?
Yes
No
< Back
Next >
Cancel

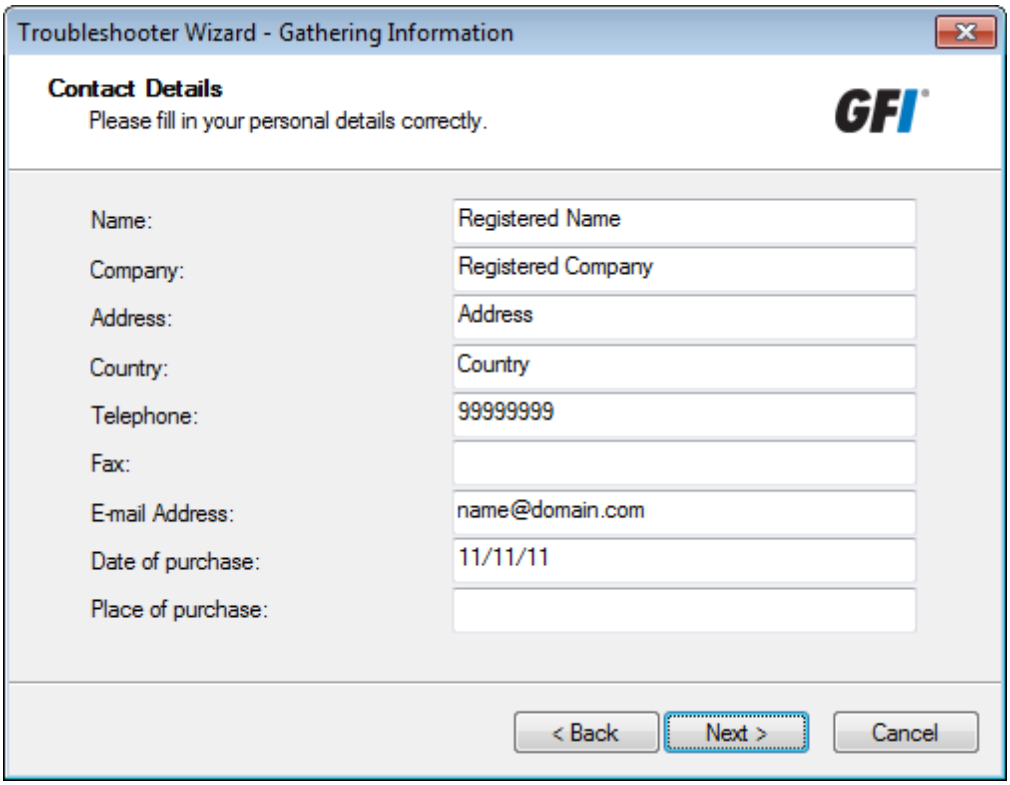
Captura de pantalla 293: Si el problema persiste, busque artículos en nuestra base de conocimiento.

7. Busque artículos relacionados con el problema en nuestra base de conocimiento. Especifique el error que experimenta en el cuadro de texto **Enter search items** y haga clic en **Search**. Si esto no resuelve el problema, haga clic en **Yes** y **Finish**. Si el problema persiste, seleccione **No** y haga clic en **Next**.


Troubleshooter Wizard - Gathering Information
More Information
The troubleshooter will collect further information.
GFI
The troubleshooter was unable to automatically locate your issue.
Next it will guide you through a wizard which will collect the information required by our support department in order to fix your issue(s).
< Back
Next >
Cancel

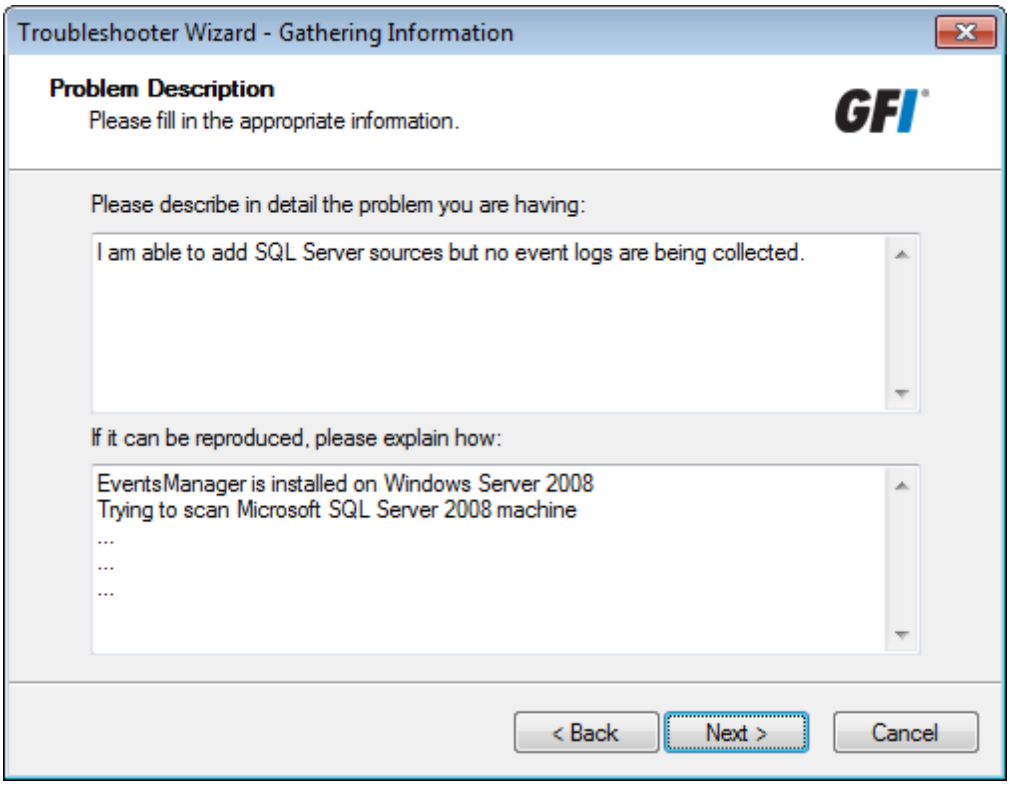
Captura de pantalla 294: Comprobar problemas manualmente

8. Haga clic en **Siguiente**.



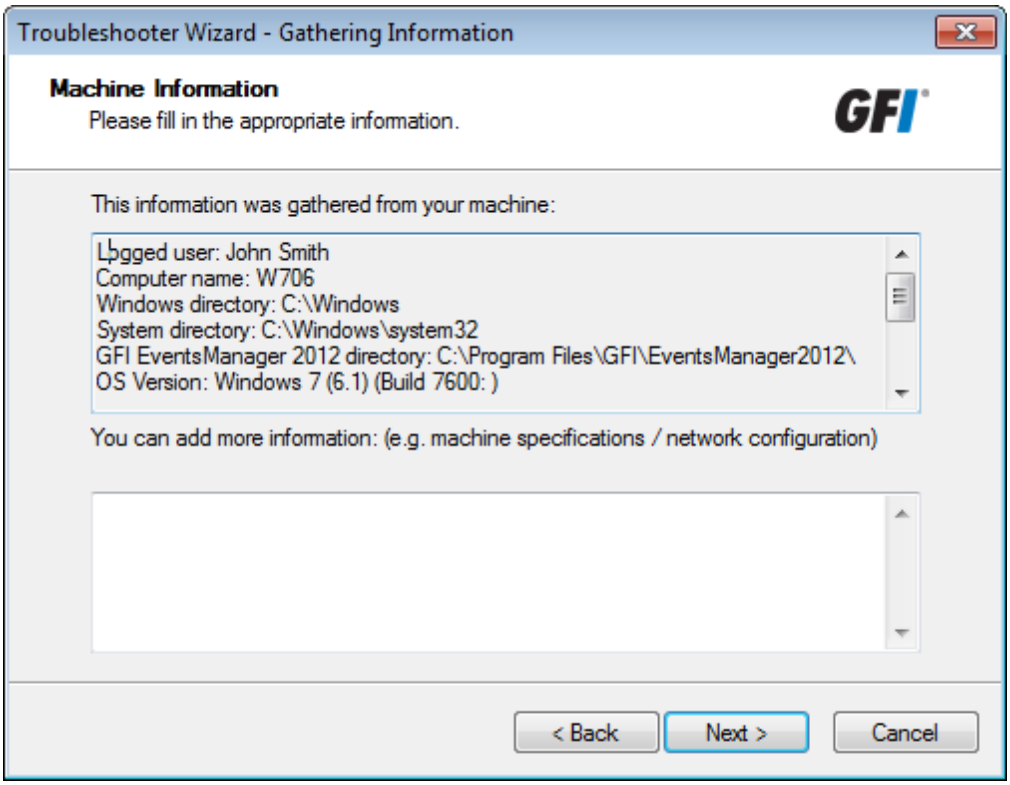
Captura de pantalla 295: Especificar detalles de contacto

9. Especifique sus datos de contacto para que nuestro equipo de soporte pueda comunicarse con usted para obtener más información. Haga clic en **Siguiente**.


Troubleshooter Wizard - Gathering Information
Problem Description
Please fill in the appropriate information.
GFI
Please describe in detail the problem you are having:
I am able to add SQL Server sources but no event logs are being collected.
If it can be reproduced, please explain how:
EventsManager is installed on Windows Server 2008
Trying to scan Microsoft SQL Server 2008 machine
...
...
...
< Back
Next >
Cancel

Captura de pantalla 296: Escribir la descripción del problema y otros datos

10. Especifique el error que se genera y otros datos que podrían ayudar a nuestro equipo de soporte a recrear este problema. Haga clic en **Siguiente**.


Troubleshooter Wizard - Gathering Information
Machine Information
Please fill in the appropriate information.
GFI
This information was gathered from your machine:
Logged user: John Smith
Computer name: W706
Windows directory: C:\Windows
System directory: C:\Windows\system32
GFI EventsManager 2012 directory: C:\Program Files\GFI\EventsManager2012\
OS Version: Windows 7 (6.1) (Build 7600:)
You can add more information: (e.g. machine specifications / network configuration)
< Back
Next >
Cancel

Captura de pantalla 297: Recopilar información de la máquina

11. El solucionador de problemas analiza su sistema para obtener información acerca del hardware. Puede agregar manualmente más información en el espacio proporcionado o hacer clic en **Next**.

Troubleshooter Wizard - Results
GFI
Completing the GFI EventsManager 2012 Troubleshooter Wizard
The file shown below is a 'ZIP' archive containing all the files that where gathered by this Wizard.
C:\Program Files\GFI\EventsManager2012\2012_04_12_203
Select 'Go to GFI Support...' for instructions on how to contact the GFI support department.
If the resulting 'ZIP' archive is larger than 4 MB, please select 'FTP Upload Instructions...' for instructions on how to upload this file to our FTP site.
FTP Upload Instructions...
Open Containing Folder...
Go to GFI Support...
< Back
Finish
Cancel

Captura de pantalla 298: Finalizar el proceso de resolución de problemas

12. En esta etapa, el solucionador de problemas crea un paquete con la información recopilada en los pasos anteriores. A continuación, se debe enviar el paquete a nuestro equipo de soporte para que pueda analizar y resolver el problema. Seleccione una de las siguientes opciones:

- **FTP Upload Instructions**: permite abrir un artículo para brindarle instrucciones acerca de cómo cargar el paquete del solucionador de problemas a nuestro servidor FTP.
- **Open Containing Folder**: permite abrir la carpeta que contiene el paquete generado por el solucionador de problemas de modo que pueda enviarlo por correo electrónico.
- **Go to GFI Support**: permite abrir la página de soporte del sitio web de GFI.

13. Haga clic en **Finish** para finalizar.

19 Glosario

A

Acciones

La actividad que se llevará a cabo como resultado de eventos que cumplen con condiciones específicas. Por ejemplo, usted puede activar acciones siempre que un evento esté clasificado como crítico. Las acciones admitidas por GFI EventsManager incluyen alertas por correo electrónico, archivado de eventos y ejecución de secuencias de comando.

Administración remota de registros de eventos

Se necesita para permitir que GFI EventsManager acceda y recopile eventos de equipos remotos. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc766438.aspx.

Alertas

Notificaciones que informan a los destinatarios que ocurrió un evento en particular. GFI EventsManager puede generar alertas por correo electrónico, por SMS y a través de la red.

Alertas a través de la red

Mensajes de red (conocidos como mensajes Netsend) que informan a los destinatarios que ocurrió un evento en particular. Estos mensajes se envían a través de un sistema/protocolo de mensajería instantánea y se muestran como una ventana emergente en la bandeja del sistema del escritorio del destinatario. Para configurar alertas a través de la red, debe especificar el nombre o IP de los equipos a los que se envían los mensajes Netsend.

Alertas por correo electrónico

Notificaciones por correo electrónico que informan a los destinatarios que ocurrió un evento en particular. Para activar las alertas por correo electrónico, debe tener acceso a un servidor de correo activo.

Alertas por SMS

Notificaciones por SMS que informan a los destinatarios que ocurrió un evento en particular. En GFI EventsManager, las alertas por SMS pueden enviarse a través de varios orígenes, incluso los teléfonos celulares con capacidades de módem y puertas de enlace basadas en Internet de correo electrónico a SMS.

Archivo

Una colección de eventos almacenados en la base de datos basada en SQL Server con copia de seguridad de GFI EventsManager.

Auditar administración de cuentas

Genera eventos cuando se realizan operaciones de administración de cuentas, como crear/eliminar una cuenta de usuario o grupo, habilitar/inhabilitar una cuenta de usuario y definir/cambiar una contraseña de usuario. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc737542(WS.10).aspx

Auditar eventos del sistema

Genera eventos cuando ocurren eventos importantes del sistema, como un usuario que reinicia o apaga el equipo de destino o cuando se produce un evento que afecta el registro de seguridad. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc782518(WS.10).aspx

Auditar seguimiento de procesos

Genera eventos que llevan a cabo un seguimiento de ciertas acciones, como los programas que se inician, se cierran, así como otra información de acceso indirecto a objetos que contengan datos de seguridad importante. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx

Auditoría de objetos

Active esta función de auditoría para auditar los eventos de usuarios que acceden a objetos (ejemplo: archivos, carpetas e impresoras). Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc976403.aspx.

B

Base de información de administración

Una MIB es el equivalente a un diccionario de datos o libro de códigos. Asocia identificadores de objetos (OID) con una etiqueta legible y otros parámetros relacionados con un objeto de red activa, como un enrutador. Su función principal es recopilar e interpretar mensajes SNMP transmitidos por los dispositivos de red habilitados con SNMP. La información almacenada en la MIB se organiza jerárquicamente y normalmente se puede acceder a ella mediante un protocolo como SNMP.

C

Capturas SNMP

Notificaciones/alertas generadas y transmitidas por los componentes de red activos (Ejemplo: hubs, enrutadores y puentes) a servidores SNMP cuando se producen eventos importantes, como errores o infracciones de seguridad. Los datos contenidos en las capturas SNMP pueden contener información de configuración, estado y estadísticas, como el número de errores del dispositivo hasta la fecha.

Carpeta de conjunto de reglas

La carpeta que contiene uno o más conjuntos de reglas.

Clasificación de eventos

La categorización de eventos de importancia crítica, alta, media, baja o ruido.

COM+ Network Access

Active este permiso de firewall para permitir que los equipos del cliente puedan acceder a aplicaciones o servicios que residen en el servidor. Esto permite a GFI EventsManager acceder a los recursos de todos los servidores. Para obtener más información acerca de este permiso, consulte http://technet.microsoft.com/en-us/library/cc731967.aspx.

Conjuntos de reglas

Una colección de reglas de procesamiento de eventos.

D

Detección de redes

Habilite este permiso de firewall para permitir que GFI EventsManager recopile información acerca de los equipos conectados a la red que se pueden analizar. Para obtener más información, consulte http://technet.microsoft.com/en-us/library/cc181373.aspx.

E

Eventos sin clasificar

Eventos que no cumplían con alguna de las condiciones de procesamiento de eventos configuradas en las reglas de procesamiento de eventos.

I

Identificador de objeto SNMP (OID)

Un identificador de objeto SNMP es una dirección compuesta por una secuencia de números «con puntos» (Ejemplo: 1.3.6.1.4.1.2682.1). Estos números identifican de forma exclusiva y localizan un dispositivo concreto (por ejemplo: hub) en toda la red. Los OID de SNMP son un componente clave en el diseño de los mensajes SNMP. De hecho, un servidor SNMP no puede interpretar o diseñar mensajes que no tengan un OID. Los proveedores individuales a menudo crean sus propias MIB que solamente incluyen los OID asociados específicamente con su dispositivo.

Internet Protocol Security

Un marco de normas abiertas utilizadas para cifrar y autenticar paquetes de red durante una sesión de comunicación entre equipos. Al utilizar servicios de criptografía, IPsec garantiza la integridad, autenticación y confidencialidad de los datos.

IPsec

Internet Protocol Security es un marco para un conjunto de protocolos de seguridad en la red o capa de procesamiento de paquetes de comunicación en red. Los abordajes de seguridad anteriores implementaron seguridad en la capa de aplicaciones del modelo de comunicaciones. Se considera que IPsec es especialmente útil para la implementación de redes privadas virtuales y el acceso de usuarios remotos a través de la conexión de acceso telefónico a redes privadas. Una gran ventaja del IPsec es que las medidas de seguridad se pueden administrar sin necesidad de implementar cambios en los equipos de los usuarios individuales.

M

Mensajes Syslog

Notificaciones/alertas generadas y transmitidas con mayor frecuencia a un servidor Syslog por UNIX y los sistemas basados en Linux cuando se producen eventos importantes. Los mensajes Syslog pueden ser generados por estaciones de trabajo, servidores y dispositivos de red acti-

vos y ciertos dispositivos, como enrutadores de Cisco y firewall Cisco PIX para registrar las errores e infracciones de seguridad, entre otras actividades.

R

Registros de eventos

Una colección de entradas que describen los eventos ocurridos en la red o en un sistema informático. GFI EventsManager admite diferentes tipos de registros de eventos, incluso: registro de evento de Windows, registro W3C, Syslog, captura SNMP y auditoría de SQL Server.

Registros de eventos de Windows

Una colección de entradas que describen los eventos que ocurrieron en un sistema informático con Windows OS.

Registros W3C

W3C es un formato de registro común desarrollado por el Consorcio de Internet. Los registros W3C son archivos planos basados en texto usados principalmente por servidores web, como Microsoft Internet Information Server (IIS), para registrar eventos relacionados con la Web, como registros web.

Reglas de procesamiento de eventos

Un conjunto de instrucciones que se aplican contra un registro de eventos.

Ruido

Entradas de registro repetidas que informan el mismo evento.

U

Uso compartido de archivos e impresoras

Active este permiso de firewall para permitir que GFI EventsManager acceda a las definiciones de eventos en los equipos de destino. Para obtener más información, consulte http://-technet.microsoft.com/en-us/library/cc779133(WS.10).aspx

20 Índice

A

Actualización automática 298

Alertas 55-56, 64, 66, 82, 139, 179-180, 193, 216, 218, 225, 234

Alertas a través de la red 221

Alertas por correo electrónico 24, 33, 179, 218, 227, 234

Alertas por SMS 222

Almacenamiento de archivos 31, 44, 53, 140, 254, 263, 291, 322

Antivirus 32, 36, 117

Archivo 25, 61, 78, 93, 113, 142, 218, 249, 262-263, 267, 308, 322, 337, 354

B

Back-end de base de datos 24, 33, 141, 252, 263, 314

Base de datos 31, 36, 47, 56, 84, 94, 103, 120, 127, 129, 136, 140, 170, 172, 176, 179, 183, 224, 252-253, 257, 260, 267, 269, 274, 278, 281, 284, 323, 332

C

Carpeta raíz 149, 158, 198, 202, 215

Clasificación 64, 66, 119, 130, 179, 187, 191, 196, 216, 308

Comprobaciones 65, 74, 81, 179, 183, 189, 196, 198, 202, 207, 213, 215, 218, 257, 354

Conjuntos de reglas 181

Consola de inicio rápido 54

Copia de seguridad 141, 295

Credenciales 42, 51, 59, 61, 64, 70, 74-76, 85, 93, 220, 245, 249, 274, 284, 299, 319

Credenciales de detección automática 249

CSV 75, 79, 108, 127, 171, 173, 335

D

DLib 38, 45, 323

DMZ 27, 29

DNS 27-28, 30, 35, 103

E

Estado 120, 138, 142-143, 168-169, 305, 334

EventsManagerAdministrator 225

Explorador de eventos 22, 31, 126-127, 130, 134, 189, 198, 245, 252, 254, 308

Exportar 31, 127, 141, 146, 170, 172, 174, 245, 252, 267, 271, 284, 292, 308, 323, 337

Exportar datos 31, 172, 263, 326

F

Firewall 22, 29, 32, 111, 340, 343, 345-346, 348-349

G

Generación de informes 127-128, 145

GFI EndPointSecurity 28, 67, 124, 171-172

GFI LanGuard 28, 119, 139, 171-172

Grupos 35, 60, 63, 69-70, 73, 80, 83, 139, 167, 178, 225, 230, 236, 239

Grupos de servidores de base de datos 84, 93

H

Hashing 255

Historial operativo 142, 164, 170, 173

I

Implementación 26, 29

Importar 36, 60, 70, 89, 98, 247, 252, 263, 267, 282, 286, 290, 308, 323, 336

Informes 56, 67-68, 147, 247, 315

Inicio de sesión 42, 51, 61, 63, 70, 76, 85, 100, 103, 121, 137, 147, 242, 274, 284, 299

Instalación 26, 30-31, 36, 45, 54, 147, 177, 299, 313, 319, 322, 331, 334, 336-337, 354

L

LAN 27-29, 257

Licencia 38, 47, 74-75, 78, 305, 319, 353

Licencias 296, 305

M

MIB 114, 182

O

Ocultación de identidad 245

Opciones de alerta 55, 64, 66, 151, 218, 235, 242, 321

Opciones de auditoría 64, 101, 242

Opciones de rendimiento 296

Operaciones de base de datos 55, 261, 271

Origen del evento 24, 80, 82, 106, 108, 186

Orígenes de eventos 24, 32, 55, 57, 61, 64-65, 69-70, 73, 75, 77, 79-81, 83, 93, 103, 111, 129, 139, 167, 169, 186, 191, 196, 200, 203, 210, 213, 218, 238, 249, 260, 306, 308, 334, 339, 347

P

Panel 56-57, 89, 99, 123-124, 127, 130, 134, 137, 165, 195, 226, 239, 241, 258, 293, 306-307, 315, 339-340, 343, 345-346

Protocolos 33, 140, 182

puertos 32, 119, 124, 140

R

Registros de eventos personalizados 118

Registros de texto 22, 24, 28, 35, 64, 75, 78, 84, 106, 109, 127, 139, 143, 182, 185, 220, 325

Reglas de procesamiento de eventos 24, 55-56, 65-66, 68, 106, 109, 112, 115, 123, 125, 130, 179, 181, 184, 193, 195-196, 201, 205, 308, 315

Resumen diario 164

S

Seguridad de la consola 63, 242-243

Servidor de base de datos DLib 38, 47

SNMP 22, 24, 33, 61, 64, 70, 75, 79, 83, 113, 140, 142-143, 170, 172, 182, 189, 196, 218, 325

Supervisar 21-22, 28-29, 34, 45, 63, 65, 68, 84, 93, 119, 125, 183, 242

Supervisión de actividades 137

Syslog 24, 30, 33, 56, 75, 83, 140, 147, 222

U

Usuarios 63, 80, 92, 119, 124, 140, 147, 151, 177, 196, 217, 225, 232, 239, 242, 298, 314

V

Vista de estadísticas 143

Vista general 138

W

WAN 27, 31

Z

Zona desmilitarizada 29

EE.UU., CANADÁ, AMÉRICA CENTRAL Y AMÉRICA DEL SUR

15300 Weston Parkway, Suite 104, Cary, NC 27513, EE.UU.

Teléfono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REINO UNIDO Y REPÚBLICA DE IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, REINO UNIDO

Teléfono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, ORIENTE MEDIO Y ÁFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Teléfono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA Y NUEVA ZELANDA

83 King William Road, Unley 5061, South Australia

Teléfono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com